GLOBAL SEMANTIC INFRASTRUCTURE (GSI)

A PROTOCOL FOR GLOBAL INTERACTION BETWEEN PROBLEMS AND SOLUTIONS

PROTOCOL • SEMANTICS • TRUST & IDENTITY • FEDERATION

GLOBAL SEMANTIC INFRASTRUCTURE (GSI)

A PROTOCOL FOR GLOBAL INTERACTION BETWEEN PROBLEMS AND SOLUTIONS

First English Edition
2026

© 2026 Sirazhudin Guseynov
All rights reserved.

ABOUT THIS BOOK

This book describes Global Semantic Infrastructure (GSI) — a global protocol that connects problems with solutions, organizations with innovators.

If AI Semantic Infrastructure (ASI) is the infrastructure of ideas, GSI is the infrastructure of interaction.

Rather than replacing ASI, it complements it by creating a dual-loop architecture in which ideas discover their requests and requests discover their answers.

CONTENTS

PREFACE

PART I. WHY GSI IS INEVITABLE

Chapter 1. Limitations of Isolated Innovation Ecosystems
Chapter 2. The Problem of Solution Discovery in the Modern World
Chapter 3. The Problem of Access for Startups, Researchers, and Independent Teams
Chapter 4. From Infrastructure of Ideas to Infrastructure of Interaction
Chapter 5. GSI as the Next Stage After the Proliferation of ASI

PART II. WHAT IS GSI

Chapter 6. GSI as a Global Interaction Protocol
- **6.1. Definition of GSI**
- **6.2. Protocol, Not Product**
- **6.3. Goals and Objectives of GSI**
- **6.4. What GSI Includes**
- **6.5. What GSI Does Not Include**
- **6.6. How GSI Connects Organizations and Individuals**
- **6.7. GSI's Dependence on ASI and Their Autonomy**

Chapter 7. GSI Applications as Protocol Clients
- **7.1. Architecture of Client Applications**
- **7.2. Analogy with the Internet and Browsers**
- **7.3. Independent Client Implementations**
- **7.4. Compatibility Between Clients**

Chapter 8. Infrastructure Participants

Chapter 9. Registration Through ASI as a Trust Mechanism
- **9.1. Why GSI Uses ASI for Identification**
- **9.2. Organizational Onboarding**
- **9.3. Individual Onboarding**
- **9.4. Role of the ASI API**
- **9.5. Baseline Trust Mechanisms**

PART III. THE RELATIONSHIP BETWEEN ASI AND GSI

Chapter 10. ASI as Local Innovation Nodes
- **10.1. Independent ASI Systems**
- **10.2. Corporate ASI**
- **10.3. Open ASI**
- **10.4. Local Idea Processing**

Chapter 11. Uniting ASI Nodes Through GSI
- **11.1. Federated Model**
- **11.2. Node Interaction**
- **11.3. Protocol Compatibility**
- **11.4. Infrastructure Scaling**

Chapter 12. Dual-Loop Architecture
- **12.1. Proactive Ideas Through ASI**
- **12.2. Problem Requests Through GSI**
- **12.3. Responses Through ASI and GSI**
- **12.4. Separation of Responsibilities**

Chapter 13. Why GSI Does Not Accept Unsolicited Ideas
- **13.1. Idea and Request as Distinct Entities**
- **13.2. The Role of ASI in Handling Ideas**
- **13.3. The Role of GSI in Handling Requests**
- **13.4. Why Mixing Systems Creates Problems**

Chapter 14. Freedom of ASI Node Connection
- **14.1. Who Can Create Their Own ASI**
- **14.2. Operator Independence**
- **14.3. Infrastructure Openness**
- **14.4. Absence of Monopoly**

Chapter 15. Self-Isolation of Violators
- **15.1. Local Blocking of Participants**
- **15.2. Isolation of Companies**
- **15.3. Isolation of ASI Nodes**
- **15.4. Federated Network Protection**

PART IV. REQUEST ARCHITECTURE

Chapter 16. The Request as the Central Object of GSI

16.1. Definition of a Request

16.2. Request Types

16.3. Request Lifecycle

16.4. The Request as a Solution Discovery Mechanism

Chapter 17. Request Creation and Structure

- 17.1. Problem Statement
- 17.2. Requirements Description
- 17.3. Constraints and Evaluation Criteria
- 17.4. Collaboration Terms
- 17.5. Additional Parameters

Chapter 18. Open and Directed Requests

- 18.1. Open Model
- 18.2. Directed Model
- 18.3. Hybrid Variants
- 18.4. Selecting the Appropriate Mode

Chapter 19. Request Categories and Routing

- 19.1. Industry Categories
- 19.2. Request Classification
- 19.3. Routing Within the Network
- 19.4. Filtering and Personalization

Chapter 20. Search and Subscription to Requests

- 20.1. Request Feed
- 20.2. Category Search
- 20.3. Industry Subscriptions
- 20.4. Notifications and Recommendations

PART V. RESPONSES AND SOLUTIONS

Chapter 21. The Response as the Primary Interaction Mechanism
- **21.1. Response Architecture**
- **21.2. The Response as a Signal of Interest**
- **21.3. The Response as a Solution Proposal**

Chapter 22. Response Format
- **22.1. Brief Solution Description**
- **22.2. Information Disclosure Level**
- **22.3. Intellectual Property Protection**
- **22.4. Supplementary Materials**

Chapter 23. Organizational Responses and Responses Through ASI
- **23.1. Organizational Responses**
- **23.2. Startup Responses**
- **23.3. Individual Responses Through ASI**
- **23.4. Interaction of the Two Infrastructures**

Chapter 24. Response Flow Limitation
- **24.1. Overload Protection**
- **24.2. Mass Distribution Restrictions**
- **24.3. Interaction Quality Control**
- **24.4. Balance of Openness and Efficiency**

Chapter 25. From Response to Collaboration
- **25.1. Establishing Contact**
- **25.2. Negotiations**
- **25.3. NDAs and Confidentiality**
- **25.4. Licensing and Partnership**
- **25.5. Joint Implementation**

PART VI. SECURITY, TRUST, AND ABUSE PROTECTION

Chapter 26. Authenticity of Requests and Responses
- **26.1. Participant Identification**
- **26.2. Cryptographic Signatures**
- **26.3. Message Authenticity Verification**

Chapter 27. Spam Protection
- **27.1. Types of Abuse**
- **27.2. Mass Distributions**
- **27.3. Irrelevant Responses**
- **27.4. Prevention Mechanisms**

Chapter 28. Complaints and Responsibility
- **28.1. Submitting a Complaint**
- **28.2. Violation Review**
- **28.3. Participant Responsibility**
- **28.4. The Role of ASI Nodes**

Chapter 29. Local Blocking of Participants
- **29.1. Blocking Companies**
- **29.2. Blocking Organizations**
- **29.3. Blocking ASI Nodes**
- **29.4. Consequences of Blocking**

Chapter 30. Self-Isolation of Violators as a Market Mechanism
- **30.1. Federated Trust Model**
- **30.2. Organizational Reputation Beyond GSI**
- **30.3. Loss of Access to Interaction**
- **30.4. Network Self-Regulation**

Chapter 31. Abuse Protection Through Complaints
- **31.1. False Complaints**
- **31.2. Competitive Attacks**
- **31.3. Balance of Participant Interests**
- **31.4. Principles of Fairness**

Chapter 32. Anonymous Interaction
- **32.1. Reasons for Anonymity**
- **32.2. International Restrictions and Regulatory Barriers**
- **32.3. Free Assistance and Solution Disclosure**
- **32.4. Limitations of Anonymous Mode**

PART VII. THE FUTURE FEDERATED NETWORK

Chapter 33. Growth in the Number of ASI Nodes
- **33.1. Emergence of Multiple Independent ASI Nodes**
- **33.2. Evolution of Innovation Ecosystems**
- **33.3. The Need for a Common Infrastructure**

Chapter 34. Compatibility Between ASI Operators
- **34.1. Interaction Standards**
- **34.2. Federated Compatibility**
- **34.3. Independence and Collaboration**

Chapter 35. Global Network of Innovation Interaction
- **35.1. A Fully Formed Ecosystem**
- **35.2. Organizations as Nodes of the Global Network**
- **35.3. New Models of Collaboration**

Chapter 36. From Accelerating Solution Discovery to Accelerating Progress
- **36.1. Reducing Communication Barriers**
- **36.2. Accelerating Technology Adoption**
- **36.3. The Global Effect of GSI**
- **36.4. Long-Term Impact on Civilizational Development**

CONCLUSION

APPENDICES

Appendix A. Example of an Open Request
Appendix B. Example of a Directed Request
Appendix C. Example of a Response to a Request
Appendix D. Example of an Individual's Response in Open and Free Mode
Appendix E. GSI Protocol Message Formats (Text Version)
Appendix F. ASI Node Responsibility Policy
Appendix G. Risks, Limitations, and Open Questions of GSI

PREFACE

This book is a continuation of the work begun in the first book on ASI.

There, we examined why the world needs an infrastructure of ideas: a system that enables every individual, team, or organization to formulate initiatives, amplify them, and transform them into structured proposals. ASI became the answer to the question: how to collect humanity's ideas and not lose them?

But as ASI evolved, it became clear:
ideas are only half of the innovation ecosystem.

The other half is interaction.
Requests.
Problems.
Needs.
Connections between those seeking a solution and those capable of creating it.

This book is about how the infrastructure of interaction emerges.
About how multiple independent ASI nodes transform into a unified network.
About how organizations begin to communicate with one another directly.
About how individuals gain access to tasks, not just to ideas.

This book is about GSI.

INTRODUCTION

This book describes GSI—Global Semantic Infrastructure—a global protocol for the interaction between problems and solutions.

If ASI is the infrastructure of proactive ideas, then GSI is the infrastructure of requests.
If ASI answers the question "What can be done?", then GSI answers the question "Who needs it?"

GSI does not replace ASI and does not compete with it.
It complements ASI, forming a dual-loop architecture:

- ASI — local innovation nodes that process ideas.
- GSI — a global network that connects organizations, ASI nodes, and participants.

This book is organized as follows:

- Part I explains why GSI is inevitable.
- Part II describes the architecture of GSI as a protocol.
- Part III shows the relationship between ASI and GSI.
- Part IV details the structure of requests.
- Part V covers the structure of responses.
- Part VI addresses security and trust.
- Part VII explores the future of the federated network.

This book does not repeat the first one.
It continues it, moving from the infrastructure of ideas to the infrastructure of interaction.

PART I. WHY GSI IS INEVITABLE

Chapter 1. Limitations of Isolated Innovation Ecosystems

The current innovation landscape consists of a set of autonomous ecosystems—corporate, startup, academic, and governmental. Each develops its own processes, tools, and infrastructure but remains confined within its own boundaries.

Corporations build internal research centers; startups create local platforms; universities publish research through academic channels; government entities formulate national programs. These systems are efficient internally but exhibit little to no cross-interaction.

This produces a fundamental problem: innovation is generated but does not connect.

Even strong solutions remain invisible to those who actually need them.

Existing interaction channels—personal networks, conferences, tenders, accelerators—do not scale and do not provide global coverage. They create fragmented, slow, and unstructured information flows that fail to enable problems and solutions to intersect.

Corporate platforms are mutually incompatible; startup ecosystems are investor-oriented rather than problem-oriented; academic databases remain isolated from industry; government systems are closed and heavily formalized.

Each ecosystem forms its own "innovation silo," disconnected from the others.

Core conclusion: innovation exists, but it is not connected.

This structural gap makes GSI inevitable as an architectural layer that must exist between all innovation ecosystems.

Chapter 2. The Problem of Solution Discovery in the Modern World

The modern world produces an immense volume of technologies, research, prototypes, and engineering developments. Yet access to these solutions remains constrained. Organizations do not know which solutions already exist, and solution creators do not know who needs them.

Solution discovery today is a manual process, reliant on informal and nonsystematic channels: personal networks, conferences, tenders, recommendations, and incidental publications. These mechanisms do not scale, cannot be automated, and fail to provide global coverage.

Even if a solution exists, a company may never become aware of it. Corporations lack a unified channel for identifying capable implementers. Startups cannot see industry demands. Researchers are unaware of the real-world problems that need solving. Government entities cannot access potential implementers due to closed procedures and rigid requirements.

Even when information about solutions is available, it remains fragmented, unstructured, and non-comparable. Marketing materials, presentations, articles, websites, and patents generate informational noise in which solutions cannot be objectively compared against one another.

Core conclusion: solution discovery has become the bottleneck of innovation. Solutions exist; problems exist—but no infrastructure directly connects them.

This is precisely what makes GSI necessary.

Chapter 3. The Problem of Access for Startups, Researchers, and Independent Teams

The world possesses vast distributed talent—startups, research groups, independent engineers—creating technologies, methods, and prototypes. Yet the majority lack access to corporations, government entities, and large organizations that could utilize their solutions.

Startups operate under conditions of opacity: they do not know what problems corporations face, what technologies industry requires, or who the potential customer is. Researchers do not know what problems exist in the real economy. Independent teams are entirely isolated from the market.

Corporations are closed, shielded by filters and internal processes. Teams are open and seeking opportunities. Between them lies an asymmetry: access is constrained, slow, and unstructured.

For a team to engage with a corporation, it must pass through accelerators, funds, tenders, intermediaries—each of which introduces additional barriers.

While the team seeks access, the market shifts, competitors advance, and corporations select alternative solutions.

Corporations cannot vet thousands of teams, so they interact only with those already "inside the system." A closed loop emerges: to gain access, one needs trust; to gain trust, one needs access.

Core conclusion: access is the primary barrier to innovation.
Talent exists; solutions exist—but access does not.

This makes GSI inevitable.

Chapter 4. From Infrastructure of Ideas to Infrastructure of Interaction

The emergence of ASI was the first step toward building a global innovation infrastructure. ASI addresses the collection, structuring, and processing of proactive ideas. But ASI does not address interaction between organizations.

An idea and a request are distinct entities.
An idea is a proactive proposal.
A request is a need.
They require different processes, different formats, and different systems.

Therefore, ASI is designed for ideas, not for requests.
ASI cannot perform the functions of task routing, implementer discovery, solution exchange, or direct organizational interaction. Attempting to embed these functions into ASI would result in overload, break the dual-loop model, and compromise architectural purity.

Centralized platforms—tender systems, accelerators, corporate portals—do not scale globally, depend on a single owner, and introduce barriers.

Interaction cannot be built on a platform. It must be built on a protocol.

Core conclusion: the world needs an infrastructure of interaction, not another platform.
And that infrastructure is GSI.

Chapter 5. GSI as the Next Stage After the Proliferation of ASI

Once ASI deployments become widespread, they will constitute a multitude of local innovation nodes.

Each ASI will operate effectively within its own scope but will have no awareness of others.

The world will have an infrastructure of ideas but will lack an infrastructure of interaction.

ASI answers the question: "What ideas exist?"
But it does not answer: "Who is capable of solving a specific problem?"

This is not a shortcoming of ASI—it is a boundary of its architecture.

Attempting to extend ASI to encompass interaction functions would break its architecture: ASI would become overloaded, companies would receive spam, and the dual-loop model would collapse.

Therefore, GSI cannot evolve from ASI—it must emerge as a separate layer.

GSI establishes a unified request language, interconnects ASI nodes, enables task routing, and forms a global interaction network.

ASI is the horizontal layer of ideas.
GSI is the vertical layer of interaction.

Core conclusion: ASI generates ideas. GSI generates interaction.
These are two layers of a single architecture.
And GSI is the inevitable next stage after the mass proliferation of ASI.

PART II. WHAT IS GSI

Chapter 6. GSI as a Global Interaction Protocol

6.1. Definition of GSI

GSI—Global Semantic Infrastructure—is a global infrastructure that unifies ASI semantic systems and enables interaction between organizations, companies,

startups, universities, research institutes, government entities, and independent teams.

GSI addresses a single specific task:
connecting the requests of some participants with the responses of those capable of fulfilling those requests.

Critically:

- GSI is not a platform,
- not a product,
- not a company,
- not a marketplace,
- not a "service."

It is a protocol and infrastructure upon which various participants may build their own systems, clients, and services.

6.2. Protocol, Not Product

GSI does not impose:

- a unified interface,
- a single application,
- a single operator,
- a single control center.

Any company, startup, or team may:

- implement their own GSI client,
- embed GSI into their internal systems,
- use GSI as a transport layer for interaction.

GSI defines only:

- message format,
- routing rules,
- identification and trust mechanisms,
- rules for handling requests and responses,
- local blocking and abuse protection mechanisms.

Everything else resides on the participant side and within their applications.

6.3. Goals and Objectives of GSI

GSI is not created as "yet another system" but as the missing infrastructure layer.

Its goals:

- enable organizations to publish requests to the global network;
- enable other participants to see these requests and respond to them;
- enable direct interaction between organizations without intermediaries or platforms;
- unite all ASI nodes into a single federated identity and trust network;
- ensure secure, scalable, and decentralized interaction.

Core premise:
GSI is infrastructure for connecting problems and solutions,
not for generating ideas.

6.4. What GSI Includes

GSI includes only those elements necessary for protocol and infrastructure operation.

1. Request and response protocol
    - request format (problem description, requirements, constraints);
    - response format (solution description, disclosure level, terms);
    - rules for "request ↔ responses" linkage.
2. Transport layer for inter-organizational interaction
    - publication of requests by organizations;
    - retrieval of requests by other participants;
    - submission of responses to requests;
    - message routing between participants.
3. Identification and trust mechanisms (via ASI)
    - participant registration exclusively through ASI;
    - use of ASI API for identity and status verification;
    - cryptographic signing of requests and responses;
    - baseline trust level for participants via their ASI nodes.
4. Federated model for ASI node interconnection
    - any ASI node may implement GSI support;
    - GSI does not manage ASI but uses them as entry points;
    - GSI does not exist "in isolation" from ASI—it relies on them as the identity layer.
5. Local blocking and self-isolation mechanisms for violators
    - local blocking of companies;
    - local blocking of ASI nodes;
    - consequences of blocking: a blocked node/company cannot see the blocking party's requests nor respond to them;
    - no global bans on ASI nodes.

6. Dual-loop separation: organizations ↔ individuals
    - organization ↔ organization: interact directly through GSI, bypassing ASI at the transport level;
    - individual ↔ organization: interaction flows through the GSI+ASI combination.

6.5. What GSI Does Not Include

It is equally important to specify what GSI does not contain.

1. GSI does not handle interfaces
    - no single "official application";
    - no UI/UX standard;
    - no requirements for client appearance.
      GSI clients may be:
    - enterprise systems,
    - web applications,
    - mobile applications,
    - integrations into existing platforms.
2. GSI does not handle idea generation
    - proactive ideas, proposals, "look at our startup," "we have a technology"—
      do not pass through GSI;
    - all initiatives go through ASI, not GSI.
      GSI operates exclusively with requests and their responses.
3. GSI does not perform AI-based content filtering
    - no built-in AI filter;
    - no centralized moderation;
    - no global ratings;
    - no "smart" recommendations.
      Filtering, recommendations, prioritization—these are functions of clients and ASI, not GSI.
4. GSI does not manage ASI and cannot ban them
    - GSI has no mechanism for global blocking of ASI nodes;
    - GSI does not determine which ASI is "good" or "bad";
    - GSI is not a regulator of ASI.
      The only mechanism is local blocking at the participant level.
5. GSI does not replace ASI
    - GSI does not handle proactive ideas;
    - GSI does not process inbound proposal flows from individuals;
    - GSI does not engage in ideation, generation, or idea analysis.
      ASI remains the infrastructure of ideas.
      GSI is the infrastructure of interaction.

6.6. How GSI Connects Organizations and Individuals

Two distinct interaction paths must be established.

6.6.1. Organization ↔ Organization (Directly Through GSI)

When a company publishes a request and another company responds:

- Company A's request → GSI → visible to other organizations;
- Company B sends a response → GSI → Company A receives the response.

In this loop:

- ASI is used only for registration and trust (via API);
- requests and responses themselves pass directly through GSI, bypassing ASI as transport.

That is:
organizations interact directly through GSI,
but their identity and access are verified through ASI.

6.6.2. Individual ↔ Organization (Through GSI and ASI)

When an individual wants to respond to an organization's request, the path always goes through the GSI+ASI combination, because a natural person cannot interact directly with organizations through GSI alone.

The process is as follows:

1. Individual sees a request in a GSI client
    - The client application displays open organizational requests obtained from GSI.
2. Individual formulates a response
    - They write a solution, proposal, or comment in their client.
3. Client sends the response to GSI
    - The response is transmitted to the GSI transport layer.
4. GSI identifies the sender type as "individual"
    - GSI cannot deliver the response directly to the organization because natural persons do not have a direct channel in GSI.
5. GSI redirects the response to the requesting organization's ASI node
    - This is the key point:
    - GSI → organization's ASI, not GSI → organization directly.
6. The organization's ASI node processes the response as a standard idea
    - To the organization, the individual's response appears as a regular inbound initiative in its ASI:

- ASI verifies the sender's identity,
- assists with structuring the response as needed,
- performs intelligent processing,
- passes it into corporate workflows.

6.7. GSI's Dependence on ASI and Their Autonomy

A delicate balance must be established:

- GSI cannot exist entirely separate from ASI,
  because entry into GSI (registration, identification, trust) occurs through the ASI API.

Yet simultaneously:

- GSI is an autonomous infrastructure,
  because requests and responses between organizations pass directly through GSI,
  without ASI participation in the transport layer.

Consequently:

- ASI — identity, trust, and human-interaction layer;
- GSI — inter-organizational interaction and request/response routing layer.

They do not merge into a single system,
but neither do they exist in isolation from each other.

Chapter 7. GSI Applications as Protocol Clients

7.1. Architecture of Client Applications

GSI applications are protocol clients that use GSI as a transport layer for publishing requests and submitting responses.

GSI does not define interface, design, or client functionality—it defines only interaction rules.

A GSI client performs three core functions:

1. Retrieving requests
   The client connects to GSI and receives the stream of requests accessible to the participant.

2. Formulating and submitting responses
   The client enables an organization to formulate a response and submit it through GSI.
3. Managing interaction
   Filters, search, sorting, local blocking of companies and ASI nodes.

Core architectural rule
Submission of a request or response to GSI is permissible only with a valid ASI API session.
Without the ASI API, the client is not authorized to perform GSI operations.
This rule is embedded in the protocol and is independent of client implementation.

7.2. Analogy with the Internet and Browsers

GSI is a protocol, not an application.
It exists in the same way the Internet exists independently of browsers.

- The Internet is a set of protocols.
- Browsers are clients that use those protocols.

Similarly:

- GSI is an inter-organizational interaction protocol.
- GSI applications are clients that use this protocol.

This model ensures:

- no monopoly,
- implementation independence,
- competition among clients,
- interface diversity,
- freedom of choice for participants.

7.3. Independent Client Implementations

GSI permits an unlimited number of independent clients, which may differ in:

- functionality,
- interface,
- architecture,
- integrations,
- target audience.

Architecturally, two client classes exist.

1) Clients for organizations (enterprise GSI clients)

These clients are designed for organizational use.
They:

- connect to GSI as a transport layer;
- use ASI only for organizational status verification (identity, permissions);
- may publish requests (tasks, needs) to GSI;
- may send direct responses to other organizations through GSI;
- have direct access to GSI transport.

Chain for an organization:
organization → enterprise GSI client → GSI → enterprise GSI client of another organization → other organization

2) Clients for individuals (user GSI clients, operating through ASI)

These clients are designed for natural persons, but architecturally they still operate through the GSI+ASI combination.

They:

- connect to GSI as a user client but lack organizational privileges;
- display to the individual organizational requests obtained from GSI;
- enable the individual to:
    - respond to a request,
    - proactively submit an idea (without request attachment);
- upon response/idea submission:
    - the client sends data to GSI,
    - GSI, knowing from registration that the sender is a natural person,
    - does not deliver the message directly to the organization,
    - but routes it to the requesting organization's ASI node;
- the organization receives this as a standard proactive idea in its ASI (without a direct "individual → organization" channel).

Chain for an individual:
individual → GSI client → GSI → organization's ASI → organization (as inbound idea in ASI)

Key point:
for individuals, GSI is:

- a display of requests (what organizations want),
- transport to the organization's ASI node,
- but not a direct channel into the organization.

Architectural distinction

- Organizations via their GSI clients:
  - publish requests,
  - receive responses,
  - interact directly with each other through GSI.
- Individuals via their GSI clients:
  - see requests,
  - formulate responses and ideas,
  - but all their messages always arrive at the organization's ASI node and are processed as proactive ideas.

Core principle:
Organizations ↔ organizations — directly through GSI.
Individuals ↔ organizations — through GSI, but always delivered to the organization's ASI node, never directly.

7.4. Compatibility Between Clients

Compatibility is ensured by the GSI protocol:

- unified request format,
- unified response format,
- unified signing rules,
- unified routing rules,
- unified access rules.

This means:

- client A may publish requests visible to clients B, C, and D;
- client E may submit a response received by client F;
- local blocking operates identically across all clients.

But access rights differ

- an organization has access to GSI operations;
- an individual does not.

This is determined not by the client but by the account type in ASI, verified through the ASI API.

Chapter 8. Infrastructure Participants

The GSI infrastructure unites all parties engaged in the global exchange of requests and solutions.

Despite the diversity of participants—companies, startups, universities, research centers, government entities, and natural persons—the GSI protocol operates with only two connection types.

These two types are determined not by GSI itself, but by the ASI system, which serves as the sole source of identity and access rights.

The first type is organizational connection.
This category includes companies, startups, universities, research institutes, and government organizations.
All register with ASI as legal entities via the ASI API.
It is the ASI API that verifies their status, provides cryptographic signing, and grants them the right to operate directly with GSI.

Organizational connection enables publishing requests, receiving responses from other organizations, and submitting own responses through GSI without ASI participation in the transport layer.
ASI in this loop serves only as a trusted registrar and identity provider, while all interaction occurs directly through GSI.

The second type is individual connection.
A natural person may register with ASI as an individual or use ASI anonymously, if permitted by the specific ASI node.
An individual may also use a GSI client, view open organizational requests, and formulate responses to them.
However, their participation in GSI always routes through ASI.

When an individual enters a response in a GSI client, the system automatically redirects that response to their ASI node.
ASI verifies identity, applies its own rules, signs the message, and only then submits it to GSI.

Thus, an individual participates in GSI but has no direct access to GSI transport and cannot publish requests or send direct responses to organizations.

This two-tier model ensures architectural purity:
organizations interact directly through GSI, while individuals interact through ASI—even when using the same client application.

Consequently, GSI remains a secure, scalable, and predictable infrastructure where participant rights are strictly determined by their ASI registration type, not by interface or client application.

Chapter 9. Registration Through ASI as a Trust Mechanism

9.1. Why GSI Uses ASI for Identification

GSI does not have its own accounts and does not perform participant registration. This is a fundamental design decision that makes the protocol independent of specific implementations and eliminates the emergence of parallel identity systems. All registration occurs in ASI because ASI possesses the semantic model of participants and the mechanisms for identity verification. ASI knows who is a natural person, who represents an organization, and what rights each participant should have. GSI accepts only those who have completed registration in ASI and fully trusts the data that ASI provides via its API. Thus, trust in GSI is not created within the protocol—it is inherited from ASI, which serves as the global attestation layer.

9.2. Organizational Onboarding

Organizations connect to GSI exclusively through the ASI API. The ASI API is provided by a specific ASI node—for example, Google ASI, Microsoft ASI, or any other ASI operator existing in the ecosystem. To obtain ASI API access, an organization undergoes an official onboarding procedure. It provides documents confirming the company's legal existence, as well as documents confirming that the specific individual performing the registration is authorized to represent that organization. Upon verification, ASI creates a corporate profile and issues the organization its API keys. These keys enable the organization to work directly with GSI: publish requests, send direct responses, and participate in global interaction. Without the ASI API, an organization cannot perform any operation in GSI, because GSI does not accept messages from unverified sources.

9.3. Individual Onboarding

Natural persons register with ASI directly, without an API. An individual creates a profile on an ASI node—for example, Google ASI—and may use the system as a verified user or as anonymous, if the ASI permits anonymous mode. If the individual has not provided identity documents, they are considered anonymous, even if they have enabled open mode. Verification of an individual is performed by submitting the required identity documents, after which ASI assigns them verified user status. An individual may use a GSI client, view open organizational requests, and formulate responses. However, their responses always route through ASI. When an individual

enters a response in a GSI client, the system automatically redirects it to the ASI node, which verifies identity, applies its own rules, signs the message, and only then submits it to GSI. An individual has no direct access to GSI transport and cannot publish requests or send direct responses to organizations.

9.4. Role of the ASI API

The ASI API is the sole mechanism through which GSI receives verified information about participant type and rights. The API informs GSI whether a participant is an organization or an individual, and based on this, GSI permits or denies specific operations. The ASI API is issued only after completing the official onboarding procedure, which includes document verification, legal status confirmation, and representative authority verification. The ASI API is not universal—each ASI node has its own onboarding rules, own document requirements, and own verification procedures. But regardless of differences between nodes, the outcome is always the same: the organization receives an API that grants it the right to operate directly with GSI. Without a valid ASI API, it is impossible to send any request or any response into GSI.

9.5. Baseline Trust Mechanisms

Baseline trust mechanisms in GSI are built on the principle that GSI does not create trust by itself but inherits it from ASI. If ASI confirms that a participant is an organization, GSI grants it direct access. If ASI confirms that a participant is an individual, GSI redirects their interaction through ASI. If ASI does not confirm a participant, GSI grants them no rights whatsoever. Thus, trust in GSI is an extension of ASI semantic identity, and GSI itself remains a pure transport protocol that operates only with those entities that have completed registration in ASI and obtained their rights through the ASI API or through user registration.

PART III. THE RELATIONSHIP BETWEEN ASI AND GSI

Chapter 10. ASI as Local Innovation Nodes

10.1. Independent ASI Systems

ASI exists as a network of independent nodes, each operating on common principles but managed by its own operator. Nodes may belong to major technology companies, universities, research centers, or government entities. Each ASI node is an autonomous system that processes ideas, manages participant registration, and

constructs semantic profiles. Node independence means there is no single center controlling the entire network. Each node defines its own moderation rules, own verification requirements, and own mechanisms for handling ideas, while maintaining compatibility with other nodes through the shared protocol. It is precisely this independence that makes ASI a scalable global system, where each node remains a local innovation center yet is capable of interacting with other nodes through GSI.

10.2. Corporate ASI

Corporate ASI nodes are established by companies that want their own infrastructure for processing ideas from employees, partners, and external participants. Such a node is fully owned by the organization and operates according to its internal policies. A corporate ASI may be closed, accessible only to employees, or open if the company wishes to accept external ideas. At the same time, the corporate ASI remains a full participant in the global network: it can connect to GSI, provide an API for organizational registration, and participate in request exchange. Corporate ASI nodes become internal innovation centers that enable companies to work with ideas systematically rather than chaotically, while maintaining control over their own data and processes.

10.3. Open ASI

Open ASI nodes are established by organizations that wish to provide broad public access to the system. These may be technology companies, universities, or independent operators. An open ASI allows natural persons to register, submit ideas, undergo verification, and participate in the global innovation ecosystem. Such nodes become entry points for millions of individuals who want to interact with organizations through GSI. Open ASI nodes ensure accessibility, transparency, and scalability, enabling any person to become a participant in the global innovation process. Each open node defines its own rules: what data is required for registration, what documents are needed for verification, and what restrictions apply to anonymous users.

10.4. Local Idea Processing

Each ASI node performs local processing of ideas, regardless of whether it is corporate or open. Local processing includes analysis, filtering, evaluation, semantic classification, and construction of the idea profile. The node may use its own models, own algorithms, and own rules, but the result is always compatible with the global network. Local processing enables nodes to operate autonomously, without transmitting ideas to other systems unless required. At the same time, ASI remains the semantic core of the entire architecture: it is here that connections are formed

between ideas, participant profiles, and contexts, which are then utilized in global interaction through GSI. Through local processing, each ASI node becomes an independent innovation center that can evolve autonomously while remaining part of the broader ecosystem.

Chapter 11. Uniting ASI Nodes Through GSI

11.1. Federated Model

The unification of independent ASI nodes through GSI is based on a federated model, in which each ASI remains fully autonomous yet remains compatible with other nodes. The federation does not create a single control center and does not require coordinated policy among ASI operators. Each node defines its own registration rules, own verification requirements, and own mechanisms for processing ideas. GSI serves only as a transport layer that connects these nodes into a single global network. The federated model enables system scaling without centralization, preserving diversity of approaches and operator independence, while providing a unified means of interaction between them.

11.2. Node Interaction

Interaction between ASI nodes through GSI occurs without direct exchange of internal data. Nodes do not transmit ideas, user profiles, or internal semantic structures to one another. Instead, they use GSI as a common layer for publishing requests and receiving responses. When an organization registered with one ASI node publishes a request through GSI, that request becomes available to all other nodes connected to the network. ASI nodes may display these requests to their users, and individuals may formulate responses that then pass through their local ASI node and are sent to GSI. Thus, interaction between nodes occurs through the shared protocol rather than through direct data exchange, preserving the privacy and autonomy of each ASI.

11.3. Protocol Compatibility

Compatibility between ASI nodes is ensured by their use of a unified interaction protocol through GSI. The protocol defines request format, response format, signing rules, routing rules, and baseline identification requirements. ASI nodes may employ different internal models, different idea-processing algorithms, and different verification mechanisms, but their interaction through GSI remains compatible due to the shared rules. This enables any ASI node to connect to the global network, regardless of who its operator is or what technologies it uses. Protocol compatibility

makes GSI a universal transport layer that unites all ASI nodes into a single ecosystem.

11.4. Infrastructure Scaling

Infrastructure scaling is achieved because GSI does not require centralization and imposes no limits on the number of ASI nodes. Each new node may join the network by implementing GSI protocol support and providing an ASI API for organizational registration. Since GSI does not store data and does not perform semantic processing, its scaling reduces to growth in participant count and traffic volume, which is addressed at the network architecture level. ASI nodes scale independently, processing ideas locally and not transmitting them to other systems. This model enables the infrastructure to grow without bottlenecks: each new node increases the overall capacity of the network rather than imposing load on a central component. Consequently, GSI becomes a global interaction layer that unites all ASI nodes, preserves their autonomy, and ensures the scalability of the entire ecosystem.

Chapter 12. Dual-Loop Architecture

12.1. Proactive Ideas Through ASI

The dual-loop architecture is built on the separation of proactive ideas and problem requests. Proactive ideas always pass through ASI, because ASI is the semantic layer capable of accepting ideas from natural persons, analyzing them, classifying them, linking them to contexts, and constructing semantic profiles. An idea submitted by an individual does not enter GSI directly, even if the user is working within a GSI client. The client transmits it to the ASI node, which performs local processing, applies its own moderation rules, verifies the sender's identity or anonymous status, and only then stores the idea in its internal system. ASI is the sole location where ideas may originate, because only ASI possesses the semantic model necessary for their interpretation. GSI does not accept proactive ideas and does not perform their processing, preserving the purity of the transport layer.

12.2. Problem Requests Through GSI

Problem requests are formulated by organizations and published through GSI as the global transport layer. Unlike ideas, requests do not require semantic processing at ingress, because they are created by organizations that have already completed registration through the ASI API and possess verified status. GSI accepts such requests directly, signed with the corporate ASI API, and makes them available to all network participants. Problem requests become global signals visible to other organizations and natural persons. They do not pass through ASI, because ASI is not

the transport layer for requests. ASI participates only in verifying organizational status, but not in routing. Thus, problem requests belong to the GSI loop, which provides global visibility of tasks and enables organizations to interact directly with one another.

12.3. Responses Through ASI and GSI

Responses in the dual-loop architecture traverse different paths depending on the sender. Organizations send responses directly through GSI, using their ASI API only for signing and status verification. Their responses do not pass through ASI at the transport level, because organizations have direct access to GSI transport. Natural persons, by contrast, do not have direct access to GSI. When an individual formulates a response in a GSI client, the system automatically redirects it to the ASI node, which verifies identity, applies its own rules, signs the message, and only then submits it to GSI. Thus, an individual's response always passes through ASI, even if the interface appears unified. This ensures security, filtering, and protection of organizations from a direct stream of messages from natural persons. Consequently, GSI receives only those responses that have passed ASI verification, and organizations receive only verified messages.

12.4. Separation of Responsibilities

The separation of responsibilities between ASI and GSI is the key element of the dual-loop architecture. ASI is responsible for semantics, identification, verification, idea processing, and participant profile management. GSI is responsible for transport, request routing, and response delivery. ASI determines who is an organization, who is a natural person, who is verified, and who is anonymous. GSI uses this information to determine access rights and interaction routes. ASI accepts ideas and processes responses from natural persons. GSI accepts requests and ensures global distribution of tasks. This separation makes the architecture resilient, scalable, and predictable: each layer performs only its own function, without interfering with the tasks of the other layer. As a result, the dual-loop model remains clean and logically consistent, enabling global interaction without mixing roles and responsibilities.

Chapter 13. Why GSI Does Not Accept Unsolicited Ideas

13.1. Idea and Request as Distinct Entities

In the dual-loop architecture, an idea and a request are two fundamentally distinct entities that belong to different layers of the system. An idea is a proactive proposal originating from an individual or organization, and it always belongs to the semantic

layer of ASI. A request is a formalized problem that an organization wants to solve, and it belongs to the transport layer of GSI. An idea cannot be sent to GSI because GSI lacks the semantic model necessary for its interpretation. A request cannot be sent to ASI because ASI is not a transport protocol for global task distribution. These two entities exist in different loops, and mixing them leads to a violation of architectural purity.

13.2. The Role of ASI in Handling Ideas

Idea handling belongs entirely to ASI, because only ASI possesses the semantic mechanisms for analysis, classification, and linking of ideas to contexts. When an individual or organization formulates a proactive idea, it is always sent to the ASI node, which performs local processing, applies its own moderation rules, verifies the sender's identity or anonymous status, and constructs a semantic profile of the idea. ASI may link ideas to one another, determine their relevance, form internal connections, and use them in subsequent interactions. GSI does not participate in this process, because it is not designed for idea processing and contains no mechanisms necessary for their interpretation. An idea is always an internal entity of ASI, and only ASI can handle it correctly.

13.3. The Role of GSI in Handling Requests

Problem requests belong to GSI, because GSI is the global transport layer that enables task distribution between organizations. Requests are created by organizations that have completed registration through the ASI API and are published directly to GSI. GSI makes these requests available to all network participants, including other organizations and natural persons. Requests do not require semantic processing at ingress, because they are formulated by professional participants who already possess verified status. GSI ensures routing, delivery, and global visibility of requests, but does not perform their analysis. This enables organizations to interact directly with one another without overloading ASI with tasks that fall outside its layer of responsibility.

13.4. Why Mixing Systems Creates Problems

If GSI were to accept unsolicited ideas, it would break the dual-loop architecture. GSI would become a chaotic stream of initiatives that it cannot process, because it lacks the semantic model. Organizations would receive a direct stream of ideas from natural persons, bypassing ASI filtering and verification, leading to spam, abuse, and loss of trust. ASI would lose its role as the semantic layer, and GSI would lose its role as the transport layer. Mixing systems would create an architectural conflict: GSI would have to perform ASI functions, and ASI would have to perform GSI functions. This would compromise the scalability, security, and predictability of the entire

infrastructure. Therefore, GSI accepts only requests, while ideas always pass through ASI, preserving the purity of the dual-loop model and ensuring correct distribution of responsibilities between layers.

Chapter 14. Freedom of ASI Node Connection

14.1. Who Can Create Their Own ASI

The ASI architecture is designed from inception so that any operator with the technical capability may create their own node. This may be a major technology company, a university, a research center, a government entity, or an independent development team. Creating an ASI node does not require obtaining permission from a central authority, because no such authority exists. It is sufficient to implement the protocols that ensure compatibility with the global network and to provide an interface for participant registration. As a result, ASI remains an open ecosystem where each new node becomes part of the broader network while retaining full autonomy. The freedom to create nodes makes ASI a distributed system in which innovation can emerge anywhere, not only in major centers.

14.2. Operator Independence

Each ASI operator is fully independent in how they organize their node's operation. They define their own registration rules, own verification requirements, own idea-processing mechanisms, and own semantic analysis models. A node may be open or closed, corporate or public, minimalist or feature-rich. Operator independence means that ASI does not become a centralized platform where all must follow uniform rules. Instead, each node evolves according to its own objectives while remaining compatible with other nodes through GSI. This model enables operators to experiment, implement their own technologies, and adapt the system to their specific needs without compromising the overall architecture.

14.3. Infrastructure Openness

The openness of ASI means that any node may connect to the global network if it implements the required protocols and ensures correct participant handling. There are no restrictions on who may become an operator, and no requirements for centralized registration. ASI nodes may emerge in different countries, across different organizations, and within different technological ecosystems. They may use their own models, own algorithms, and own approaches to idea processing, while remaining part of a unified network through GSI compatibility. Openness makes the infrastructure resistant to monopolization and enables it to grow organically, without dependence on a single provider or a single company.

14.4. Absence of Monopoly

The absence of monopoly is a fundamental property of the ASI and GSI architecture. Since any operator may create their own ASI node, and connection to GSI does not require centralized permission, the system cannot be captured by a single company or state. Even if a major operator establishes a powerful ASI node, other participants may develop their own nodes, offering alternative models, interfaces, and rules. GSI unites all nodes into a single network but does not control or manage them. This makes the infrastructure resilient, distributed, and free from dependence on a single center. The absence of monopoly enables the system to evolve naturally, maintaining a balance between node independence and global compatibility through GSI.

Chapter 15. Self-Isolation of Violators

15.1. Local Blocking of Participants

Self-isolation of violators in the infrastructure is built on the principle of local blocking, where each organization or ASI node independently decides with whom to interact. If a participant violates rules, abuses the system, or creates a threat, an organization may block them at its own level. Such blocking does not require coordination with other participants and does not automatically propagate across the entire network. Local blocking means that a blocked participant cannot submit responses or interact with the organization that blocked them, even if they remain active in other parts of the network. This creates a mechanism of natural self-isolation, where a violator loses access to those unwilling to work with them, but does not affect the operation of the broader ecosystem.

15.2. Isolation of Companies

Isolation of companies operates on the same principle as individual participant blocking, but at the organizational level. If a company violates interaction rules, abuses requests, submits low-quality responses, or acts in bad faith, other companies may locally block it. After blocking, the company cannot see the requests of those organizations and cannot send them responses. Since GSI is a transport layer, it does not intervene in these decisions and does not impose centralized rules. Each organization independently determines whom it considers a trustworthy partner. As a result, a violator gradually becomes self-isolated: the more organizations block them, the fewer requests they see and the fewer opportunities remain for participation in global interaction through GSI.

15.3. Isolation of ASI Nodes

ASI nodes may also be isolated if they violate ecosystem rules—for example, by permitting mass abuse, failing to provide participant verification, or deliberately distorting data. Since each ASI node is an independent operator, other nodes may decide not to interact with it. Such isolation means that requests published through that node will not be displayed in other nodes, and responses from its users will be ignored. GSI does not prohibit the node from connecting, but other participants may locally disable interaction with it. This creates a natural self-regulatory mechanism, where non-compliant nodes lose access to the global network without affecting the operation of the rest. Node isolation does not require centralized management and does not violate the federated model, in which each operator remains autonomous.

15.4. Federated Network Protection

Federated network protection is based on the principle that blocking decisions are made locally, but their cumulative effect forms global resilience. Since any participant—whether an organization, an individual, or an ASI node—may be blocked independently, a violator gradually becomes self-isolated even if formally remaining part of the network. The federated model does not permit global bans, centralized sanctions, or a single authority that decides who is entitled to participate in the system. Instead, the network protects itself through distributed decisions by numerous independent operators. If a participant behaves correctly, they remain part of the ecosystem. If they violate the rules, they lose access to those unwilling to interact with them. This model makes the network resilient, self-regulating, and protected against abuse, while preserving the freedom of connection and absence of monopoly that are fundamental properties of ASI and GSI.

PART IV. REQUEST ARCHITECTURE

Chapter 16. The Request as the Central Object of GSI

16.1. Definition of a Request

The request is the central object of the GSI infrastructure because it initiates the process of global interaction between organizations and natural persons. A request is a formalized description of a problem, task, or need that an organization wants to solve. It is created exclusively by a participant registered in ASI as an organization and is signed through its corporate ASI API. A request is not an idea and does not contain solution proposals; it represents a pure description of a problem that the organization is willing to open for external interaction. GSI accepts requests directly

because they do not require semantic processing at ingress and are already structured by professional participants at origin.

16.2. Request Types

Requests in GSI may span different domains, but all conform to a single model: they are always formalized problems, not proactive proposals. A request may describe a technical task, a research problem, an infrastructure challenge, a business question, or a social need. The request type is determined by the organization itself, but its structure remains common across the entire network, ensuring compatibility between ASI nodes and correct routing through GSI. Regardless of content, each request is a signal that propagates across the network and becomes visible to other organizations and natural persons. Request types do not require classification within GSI, because GSI does not perform semantic processing; their interpretation occurs at the participant level, where they are read and analyzed independently.

16.3. Request Lifecycle

The request lifecycle begins at the moment of publication by an organization through the corporate ASI API. After signing, the request is transmitted to GSI, where it becomes available to all network participants. Natural persons may view requests through their ASI nodes, while organizations may view them directly through GSI. Responses to requests flow back into GSI, but the response path depends on participant type: organizations send responses directly, while natural persons send them through ASI. A request remains active until the organization closes or deletes it. GSI does not intervene in request content, does not evaluate its relevance, and does not manage its status; all decisions are made by the organization that published it. Thus, the request lifecycle is fully controlled by the initiator, while GSI provides only transport and global visibility.

16.4. The Request as a Solution Discovery Mechanism

The request is a solution discovery mechanism because it creates an entry point for interaction between organizations and natural persons. Unlike proactive ideas, which originate in ASI, requests form the problem loop that requires external participation. Requests enable organizations to find solutions outside their internal structures, engaging experts, researchers, startups, and individuals. Through GSI, requests become global signals that can be seen anywhere in the network, regardless of which ASI node the participant is registered with. This transforms GSI into a mechanism for global solution discovery, where every problem has a chance to be noticed by those capable of offering a response. Requests create an interaction structure in which ASI processes ideas and responses from natural persons, while

GSI provides transport and task visibility, preserving the purity of the dual-loop architecture.

Chapter 17. Request Creation and Structure

17.1. Problem Statement

Request creation in the GSI infrastructure begins with a problem statement, which must be as precise, concise, and free from assumptions about possible solutions as possible. The organization describes only what it wants to change, improve, or investigate, without proposing implementation options or imposing a direction of thought. The problem statement is a pure description of a situation requiring external participation. It contains no technical details, collaboration terms, or selection criteria. This is the starting point that defines the request's meaning and makes it comprehensible to all network participants, including natural persons, startups, and other organizations. The problem statement is created by the organization, but its identifier and signature are automatically generated by the ASI node, eliminating the possibility of forgery or request submission on behalf of another company.

17.2. Requirements Description

Following the problem statement, the organization describes the requirements that define what the solution must be. Requirements include technical parameters, functional expectations, material constraints, operational conditions, or any other characteristics necessary for correct task execution. This field is standardized to eliminate ambiguity and ensure predictability for responders. Requirements are not a solution proposal; they define the boundaries within which the solution must exist. The ASI node does not interpret requirements but only verifies structural correctness. GSI transmits them as-is, performing no semantic processing. Thus, requirements become part of the formal task description available to all network participants.

17.3. Constraints and Evaluation Criteria

Constraints define the boundaries within which the solution must operate. These may be time frames, legal restrictions, environmental requirements, budget limits, or any other conditions that cannot be violated. Evaluation criteria define how the organization will select the best response. They may include efficiency, cost, innovativeness, implementation speed, or other parameters important to the request initiator. Constraints and evaluation criteria are mandatory fields because without them the request becomes incomplete and may lead to misunderstanding of the

task. ASI records these fields in structured form, and GSI delivers them to all network participants without alteration.

17.4. Collaboration Terms

Collaboration terms are a central element of the request structure because they define the basis on which the organization is willing to interact with responders. Terms are selected exclusively from a standardized set, which includes options ranging from pro bono participation to joint intellectual property ownership. The organization may specify multiple terms simultaneously, but this does not mean all must be fulfilled. Multiple terms represent a set of possible collaboration forms from which the responder chooses one. If the terms include parameters such as payment amount or percentage share, these values become binding. A responder always has the right to submit a solution free of charge, even if the request does not contain such an option. An anonymous response—from an individual or organization—is automatically considered free and without attribution, because anonymity precludes the legal possibility of payments, shares, or joint ownership of the result.

17.5. Additional Parameters

Additional parameters allow the organization to include structured information that helps the responder better understand the task. These may be technical specifications, documentation links, examples, diagrams, or data formats. These parameters are not mandatory, but they must be presented in structured form so that ASI nodes can process them correctly. Additional parameters do not replace requirements and cannot contain collaboration terms. They serve as an extension of the request that makes the task more comprehensible but does not change its essence. GSI transmits this data without interpretation, preserving it in the form provided by the organization.

Chapter 18. Open and Directed Requests

18.1. Open Model

The open request model is based on the principle of global visibility. When an organization publishes an open request, it becomes accessible to all network participants: natural persons, startups, research groups, and other organizations. The open request propagates through GSI as a general signal that can be seen at any ASI node, regardless of country, industry, or participant scale. The open model creates maximum competition and maximum probability that a solution will be found. It is suitable for tasks where diversity of ideas, response speed, and a broad range of possible approaches are important. An open request does not assume

privacy: all participants see the collaboration terms, evaluation criteria, and constraints. Responses may be either verified or anonymous, and anonymity does not restrict access to the request. The open model transforms a task into a global challenge accessible to anyone capable of proposing a solution.

18.2. Directed Model

The directed request model is intended for situations where an organization wants to interact not with all network participants, but only with specific recipients. A directed request is visible only to those organizations or individuals to whom it is addressed. This may be due to confidentiality, industry specificity, legal constraints, or the need to work with trusted partners. The structure of a directed request is identical to that of an open request: it contains a problem statement, requirements, constraints, criteria, and standardized collaboration terms. The difference lies solely in visibility. A directed request is not private in the technical sense—it still passes through GSI—but access to it is restricted at the level of the recipients' ASI nodes. Responses to a directed request may be either open or anonymous, and anonymity does not violate the model because the initiator sees only the response content, not the sender's identity. The directed model creates controlled interaction while maintaining architectural compatibility with the open model.

18.3. Hybrid Variants

The hybrid model arises when an organization wishes to combine the advantages of both open and directed schemes. In this case, the request may be published as open but with an additional directed layer aimed at specific participants who possess particular competencies and resources. A hybrid request is visible to all, but certain participants receive priority notification or extended interaction parameters. This model enables the organization to simultaneously attract a broad audience and work with a narrow circle of experts. The hybrid model does not change the request structure and does not create new object types. It merely extends delivery mechanisms and makes interaction more flexible. Responses to a hybrid request are processed the same as for any other: the responder selects one of the proposed collaboration terms or may submit a solution free of charge. Anonymous responses remain free and without attribution, regardless of whether the request was open, directed, or hybrid.

18.4. Selecting the Appropriate Mode

The choice between open, directed, and hybrid modes depends on how the organization wishes to interact with the ecosystem. If the task requires maximum reach, diversity of ideas, and high response speed, the open model is used. If the task involves confidentiality, industry specificity, or the need to work with trusted

participants, the directed model is applied. If the organization wants to combine the advantages of both schemes, it chooses the hybrid mode. Importantly, the request structure remains unchanged in all three cases; only visibility differs. This makes the system predictable, compatible, and robust. Regardless of mode, the responder always has the right to select one of the proposed collaboration terms or to submit a solution free of charge. Anonymous responses remain free and without attribution, ensuring legal clarity and protection for all parties. Thus, mode selection affects only the audience, not the interaction architecture.

Chapter 19. Request Categories and Routing

19.1. Industry Categories

Industry categories serve as the basis for primary request structuring within GSI. They do not determine request content and do not affect its structure, but they enable ASI nodes to efficiently distribute information flows. Categories create a context in which the request becomes part of a broader industry landscape: engineering, biotechnology, energy, education, healthcare, transportation, or any other domain. A category does not restrict access to the request and does not filter participants; it merely helps the system navigate the scale of the global network. Industry categories are standardized to eliminate duplication and ensure compatibility between ASI nodes across different countries and organizations. They enable participants to quickly find requests relevant to their competencies and form the basis for further routing.

19.2. Request Classification

Request classification in GSI is not semantic processing. The system does not attempt to understand the meaning of the task and does not interpret its content. Instead, classification is based on structural attributes: industry category, task type, collaboration terms, and additional parameters. Classification serves as a tool for search optimization and filtering, not for analysis. It enables participants to quickly navigate large volumes of requests and find those that match their interests, competencies, or capabilities. Classification does not affect request visibility: open requests remain accessible to all, while directed requests remain accessible only to their intended recipients. Thus, classification is an auxiliary mechanism that makes interaction more convenient but does not change the GSI architectural model.

19.3. Routing Within the Network

Request routing within GSI is based on the principle of minimal intervention. The system does not analyze request content and does not make decisions about to whom it should be shown. It merely ensures delivery of the request to those ASI nodes that have the right to see it. In the case of open requests, routing is global: the request propagates across the entire network and becomes accessible to all participants. In the case of directed requests, routing is restricted to the specific nodes specified by the initiator. Hybrid requests combine both approaches: they are visible to all, but certain participants receive priority notification. Routing does not depend on collaboration terms, evaluation criteria, or additional parameters. It is based solely on request type and category. This makes the system predictable, robust, and scalable, enabling it to handle millions of requests without overload.

19.4. Filtering and Personalization

Filtering and personalization occur at the ASI node level, not within GSI. Each participant—whether an individual or an organization—accesses requests through their ASI node, which takes into account their competencies, interests, interaction history, and selected domains. ASI does not hide requests if they are open, but it may elevate relevant requests higher in the display to improve interaction quality. Personalization does not affect GSI architecture and does not change request visibility. It merely helps the participant navigate large volumes of information. Filtering also allows hiding requests that do not match selected collaboration terms or industry interests, but this occurs only on the participant side. Thus, filtering and personalization make interaction more convenient without violating the principles of openness and transparency embedded in the GSI architecture.

Chapter 20. Search and Subscription to Requests

20.1. Request Feed

The request feed is the primary interface through which a participant interacts with the global GSI network. It is formed at the ASI node level and represents a continuous stream of open requests arriving from organizations worldwide. The feed does not hide information and does not restrict access: every open request appears in it immediately upon publication. At the same time, the feed is not static—the participant may configure its display according to formal parameters without violating openness principles. They may sort requests by publication date, filter them by industry category, by collaboration terms, or by initiating organization names. These settings do not alter the feed itself and do not affect request visibility; they

merely enable the participant to organize the information flow so that it aligns with their interests, competencies, or current tasks. The feed remains a global space of opportunities, and settings transform it into a manageable navigation tool within that space.

20.2. Category Search

Category search complements the request feed and enables the participant to quickly find tasks relevant to specific domains. Search operates exclusively on formal parameters—industry category, request type, collaboration terms, and structured fields. It does not perform semantic analysis and does not attempt to interpret the meaning of the task. This makes search fast, predictable, and scalable. The participant may search for requests in engineering, biotechnology, education, or any other field, combining categories with collaboration terms or constraints. Search does not restrict access to requests and does not hide them; it merely helps structure information while preserving the openness and transparency principles embedded in the GSI architecture. Thus, category search becomes a tool for precise navigation within the global task space.

20.3. Industry Subscriptions

Industry subscriptions enable the participant to receive notifications about new requests in selected domains. A subscription does not create private channels and does not change request visibility; it merely forms a personalized notification stream at the ASI node level. The participant may subscribe to one or more industries, and ASI will automatically notify them about new requests belonging to those categories. Subscriptions do not affect routing and do not alter request structure. They serve as a convenience tool, allowing the participant not to miss tasks that match their competencies or interests. Subscriptions may be temporary or permanent, and the participant may modify them at any time. Thus, industry subscriptions create a personalized layer on top of the global feed, preserving GSI architectural principles and providing convenient navigation within the ecosystem.

20.4. Notifications and Recommendations

Notifications and recommendations are formed at the ASI node level and are based on the participant's interaction history, competencies, selected subscriptions, and preferred collaboration terms. Notifications inform the participant about new requests, changes to existing tasks, or responses to their own solutions. Recommendations are not algorithmic predictions and do not attempt to impose specific tasks on the participant. They merely elevate relevant requests higher in the display while maintaining access to the entire feed. Notifications and recommendations do not affect request visibility and do not restrict access to them.

They serve as navigation tools that make interaction with GSI more convenient but do not change the network's architectural model. Thus, notifications and recommendations create a personalized layer on top of the global request space, preserving the principles of openness, transparency, and equal access.

PART V. RESPONSES AND SOLUTIONS

Chapter 21. The Response as the Primary Interaction Mechanism

21.1. Response Architecture

The response is a fundamental element of interaction within GSI. If a request is an organization's initiative, then a response is a participant's action expressing their willingness to engage. The response architecture is designed to be simultaneously simple, flexible, and legally clean. A response contains only what is necessary for evaluation: the selected collaboration term, the solution content, and the sender's status—anonymous or verified. The ASI node automatically records the response identifier, verifies structural correctness, and transmits it to the request initiator. A response does not require contract registration, does not create legal obligations, and does not imply automatic acceptance. It is a proposal that the organization may review, reject, or develop further. The response architecture is minimalist because its purpose is to provide a clean channel for solution transmission, unburdened by extraneous data and requiring no interpretation.

21.2. The Response as a Signal of Interest

A response in GSI is not only a solution to a task but also a signal of interest. Even if a participant does not provide a complete solution, the mere fact of responding demonstrates their willingness to interact, discuss, clarify, or develop the idea. A response may be brief, preliminary, or even incomplete, yet it is still recorded by the system as an expression of interest. This is particularly important in open requests, where an organization may receive dozens or hundreds of replies. A response becomes an indicator that the participant sees value in the task and is willing to offer their contribution. In directed requests, the response carries even greater weight because it demonstrates the willingness of a specific participant to enter into dialogue. Thus, the response serves a dual function: it conveys solution content and simultaneously acts as an engagement marker that helps the organization navigate the flow of replies.

21.3. The Response as a Solution Proposal

A response is a solution proposal that the participant formulates based on the requirements, constraints, and collaboration terms specified in the request. The participant selects one of the proposed terms, or may submit a solution free of charge even if the request does not contain such an option. This makes the model flexible and protects the author's freedom. An anonymous response is always considered free and without attribution, ensuring legal clarity and precluding the possibility of obligations arising. The solution content may be complete, partial, or conceptual—the system does not restrict the format as long as it conforms to the response structure. The organization reviews the solution, compares it with other replies, and makes a decision regarding further interaction. A response is not a contract and does not create obligations; it merely opens the possibility of collaboration. Thus, the response becomes the primary mechanism through which participants offer their ideas, knowledge, and developments, forming a dynamic interaction ecosystem within GSI.

Chapter 22. Response Format

22.1. Brief Solution Description

The response format in the GSI infrastructure is designed so that the request initiator can quickly understand the essence of the proposed solution without spending time analyzing excessive detail. Therefore, every response begins with a brief solution description—structured, precise, and focused on the core. This description is not advertising, a presentation, or an attempt to persuade the organization; it serves as a technical summary that enables assessment of the line of reasoning and compliance with requirements. The brief description should reflect the key idea, method, or approach proposed by the participant, but is not required to disclose internal mechanisms or unique development elements. It creates context for further analysis and enables the organization to quickly compare responses against one another. The ASI node records this field as mandatory, because without it the response loses structural integrity and becomes difficult to process.

22.2. Information Disclosure Level

The level of information disclosure in a response is determined by the participant themselves. The system does not require full disclosure of the solution and does not impose a format that could lead to loss of intellectual property. The participant may provide either a complete solution or a partial, conceptual, or demonstration-level one. They may limit themselves to describing the approach, indicating direction, or

providing a minimal data set sufficient for evaluation. This is particularly important in cases where the request involves solution acquisition, licensing, or joint development. The participant determines what volume of information is safe to disclose prior to contract execution. GSI does not analyze response content and does not evaluate completeness of disclosure; it merely transmits the data in the form submitted by the participant. Thus, the disclosure level becomes both a tool for author protection and a means of demonstrating competence.

22.3. Intellectual Property Protection

Intellectual property protection is embedded in the GSI architecture and does not require additional actions from the participant. If a response is sent anonymously, it is automatically considered free of charge and without attribution, which eliminates legal risks and makes the solution freely usable. If a response is sent by a verified participant, they retain all rights to their solution until an agreement is executed within the framework of the selected collaboration term. Even if the participant provides a partial solution or a demonstration fragment, this is not considered a transfer of rights. GSI is not a mechanism for intellectual property transfer; it is merely a communication channel. Rights transfer occurs only within the terms selected by the participant and only after agreement with the organization. Thus, the response format ensures a balance between openness and protection, enabling participants to share ideas without risk of losing control over them.

22.4. Supplementary Materials

Supplementary materials are an optional part of the response, but they can significantly increase its value. The participant may attach diagrams, calculations, examples, research links, demonstration files, or any other structured data that helps better understand the proposed solution. These materials do not replace the brief description and are not mandatory for all task types. They serve as an extension of the response, allowing the participant to show depth of elaboration or demonstrate the technical viability of their approach. The ASI node accepts supplementary materials in any format that meets technical requirements and transmits them to the request initiator without alteration. Supplementary materials do not affect the legal status of the response and do not create obligations. They merely help the organization evaluate the solution more thoroughly and make an informed decision about further interaction. Thus, supplementary materials become a tool for strengthening the response while preserving the architectural purity and flexibility of the format.

Chapter 23. Organizational Responses and Responses Through ASI

23.1. Organizational Responses

Organizational responses are a key element of interaction within GSI, because it is organizations that possess the resources, infrastructure, and capability to implement solutions at industrial scale. When an organization submits a response, it passes through its ASI node, which verifies its status, checks structural correctness, and records the selected collaboration term.

A verified organizational response is transmitted directly through GSI, bypassing ASI as a transport layer. It contains the organization's identifier and enables the request initiator to immediately understand whom they are interacting with.

An anonymous organizational response, like any other anonymous response, passes through the ASI node, which provides filtering and structuring. The ASI node does not disclose the sender's identity and does not know who exactly submitted the anonymous response. An anonymous response is always considered free of charge, eliminating the need for contract execution and making interaction safe for both parties.

Thus, organizational responses—whether strategic or exploratory—preserve architectural purity and flexibility while maintaining clear separation between verified and anonymous channels.

23.2. Startup Responses

Startup responses occupy a special place in the GSI ecosystem, because startups are most often the ones offering unconventional approaches, rapid prototypes, and innovative solutions. Startups use the same mechanisms as larger organizations: their responses pass through the ASI node, are recorded by the system, and are delivered to the request initiator. However, startups more frequently choose collaboration terms related to joint development, product equity, or licensing, because these models enable them to develop their own technologies.

A startup may submit a verified response, which contains its identifier and allows the initiator to assess partnership potential. A startup may also submit an anonymous response if it wishes to conceal its strategy or is testing a hypothesis. Such a response, like any anonymous response, passes through the ASI node, undergoes filtering, and is considered free of charge.

Thus, startups become a dynamic element of the network, providing an influx of new ideas and technologies through both verified and anonymous channels.

23.3. Individual Responses Through ASI

Natural persons interact with GSI exclusively through ASI nodes, which provide their identification, data protection, and response structuring. An individual may submit a response either verified or anonymously.

A verified response allows authorship to be retained, collaboration terms to be selected, and participation in legally significant models such as solution acquisition or licensing.

An anonymous response is always considered free of charge and without attribution, making it safe for both parties. The ASI node provides filtering and structuring but does not disclose or store the sender's identity.

Individuals often submit partial solutions, concepts, or ideas that may become the foundation for further development. ASI ensures the structural correctness of the response and transmits it to the request initiator without alteration. Thus, natural persons become full participants in the global ecosystem, capable of influencing the development of technologies and solutions on par with organizations.

23.4. Interaction of the Two Infrastructures

The interaction between ASI and GSI is the foundation of the entire response architecture. ASI is responsible for identification, structuring, verification, filtering, and delivery of responses, while GSI provides global routing and connectivity between participants.

A response is always created within ASI. For verified responses, ASI knows the sender, their status, and their rights. For anonymous responses, ASI provides filtering and structuring but does not disclose or store the sender's identity.

GSI does not analyze response content and does not store sender information; it merely transmits data between nodes. This separation of roles ensures security, scalability, and legal clarity.

An organization, startup, or individual interacts with GSI only through ASI, and it is precisely this that makes the system resistant to abuse. Verified responses retain authorship and enable agreements to be concluded, while anonymous responses remain free of charge and create no obligations.

Thus, the interaction of the two infrastructures forms a unified mechanism in which responses become the primary means of transmitting knowledge, ideas, and solutions.

Chapter 24. Response Flow Limitation

24.1. Overload Protection

Response flow limitation in GSI is based not on filtering or relevance evaluation, but on an architectural principle: each organization may submit only one response per request. This rule is embedded in the ASI node and eliminates the possibility of mass replies or attempts to overwhelm the customer with dozens of messages. A response from an organization always goes directly through its ASI node to the request initiator, bypassing any intermediate checks. ASI guarantees only structural correctness, but does not evaluate content. This means the system does not attempt to determine whether a response is relevant—the only one who can do that is the customer themselves. This approach protects the network from overload while preserving the principle of openness.

24.2. Mass Distribution Restrictions

The "one response per request" mechanism completely eliminates mass distributions. An organization cannot send the same response to multiple requests, because each response is tied to the specific request identifier automatically generated by the initiator's ASI node. Attempts to send duplicate responses are blocked at the sender's ASI node level. The system does not analyze response meaning and does not check its quality, but it guarantees that an organization cannot use GSI as a channel for spam. If an organization attempts to abuse the system by submitting irrelevant responses, the only control mechanism is the customer's reaction. This makes the architecture simple, transparent, and resistant to abuse.

24.3. Interaction Quality Control

Quality control in GSI is performed not by the system, but by the customer themselves. If a customer receives a response that is spam, abusive, or an attempt at manipulation, they may file a complaint against the responder. The complaint is transmitted to the ASI node of the sending organization, and it is that node that decides whether to revoke the ASI API. If the node does not respond or ignores the complaint, the customer has the right to independently block the specific responder or the entire ASI node to which they belong. Blocking means that the customer no longer sees requests from that node and cannot receive responses from it. This creates a natural self-regulatory mechanism: ASI nodes are incentivized to ensure their clients do not abuse the system, otherwise they lose trust and access to the ecosystem.

24.4. Balance of Openness and Efficiency

The balance between openness and efficiency is achieved because GSI does not intervene in response content and does not attempt to evaluate its relevance. The system remains fully open: any organization may respond to any open request. But efficiency is ensured by strict architectural constraints: one response per request, direct channel through the ASI node, complaint mechanism, and blocking mechanism. If an organization sends a response such as "we have a solution to your problem," and after contact it turns out there is no solution or the response was irrelevant, the customer files a complaint, and the ASI node is obligated to revoke the offender's ASI API. If the node fails to do so, the customer blocks the node independently. Thus, the system remains open but does not permit abuse, maintaining high interaction quality without the need for global moderation or content analysis.

Chapter 25. From Response to Collaboration

25.1. Establishing Contact

The transition from response to collaboration begins when the request initiator decides to contact the participant who submitted the solution. Contact is established directly, without GSI involvement and without ASI node intermediation. The system does not regulate this stage and does not intervene in communication: it merely ensures response delivery and provides the initiator with the ability to contact the sender if the latter chose verified status. If the response was anonymous, contact is impossible, because anonymity precludes data exchange. Establishing contact is the first step in which interaction moves beyond the GSI infrastructure and enters the realm of direct communication between parties. At this stage, the request initiator evaluates the seriousness of intent, competence, and the participant's readiness for further interaction.

25.2. Negotiations

Negotiations occur entirely outside GSI and are not recorded by the system. They may include discussion of solution details, requirement clarification, timeline coordination, role distribution, or work scope definition. Negotiations are not constrained by the response format and may develop in any direction acceptable to both parties. GSI does not provide negotiation tools and does not intervene in their content. This enables participants to freely shape the terms of future collaboration without violating the network's architectural principles. Negotiations become the

bridge between solution proposal and the formation of a real partnership, while preserving full autonomy for both parties.

25.3. NDAs and Confidentiality

If the parties move to discussing details that require protection, they may enter into a non-disclosure agreement (NDA). GSI does not provide built-in mechanisms for exchanging confidential information and does not participate in the legal execution of NDAs. All data protection matters are handled directly between participants. An NDA becomes the point at which interaction moves beyond the open model and transitions into a protected format. This is particularly important in cases where the responder provided only the conceptual part of the solution and is willing to disclose details only after signing the agreement. Thus, an NDA serves as a legal instrument that enables parties to safely exchange information without violating GSI's architectural purity.

25.4. Licensing and Partnership

Following negotiations, the parties may proceed to formalizing the legal model of collaboration. This is determined by the term selected by the participant—licensing, solution acquisition, joint development, joint intellectual property, or product equity. GSI does not participate in contract execution and does not record legal relationships between parties. All agreements are formalized outside the system, and GSI remains only the entry point through which the parties found each other. Licensing and partnership become the outcome of negotiations, not part of the network architecture. This allows GSI to remain a neutral infrastructure, uninvolved in legal processes.

25.5. Joint Implementation

Joint implementation is the stage at which the solution transforms into a product, technology, or service. This stage lies entirely outside GSI and is not recorded by the system. Implementation may include joint development, technology integration, prototype creation, testing, manufacturing, or product market launch. GSI does not track progress, does not monitor obligation fulfillment, and does not intervene in the process. The system has fulfilled its task at the moment the request initiator received a response and established contact with the participant. Everything beyond that is the responsibility of the parties, who independently determine the format, timeline, and mechanisms of implementation. Thus, GSI remains an infrastructure for discovery and connection, not a project management platform.

PART VI. SECURITY, TRUST, AND ABUSE PROTECTION

Chapter 26. Authenticity of Requests and Responses

26.1. Participant Identification

The authenticity of requests and responses in the GSI infrastructure is ensured through strict participant identification at the ASI level. Any organization, startup, or individual interacts with the network only through their ASI node, which verifies their status and guarantees that the message genuinely originates from the stated sender. ASI does not disclose personal data and does not transmit identity into GSI, but it does confirm the fact of sender authenticity. This means that organizational requests cannot be forged: only their own ASI node has the authority to sign and send such messages. The same applies to responses—the system does not permit sending a response on behalf of another company or individual. Thus, identification becomes the fundamental trust layer upon which the entire interaction architecture is built.

26.2. Cryptographic Signatures

Every request and every response in GSI is accompanied by a cryptographic signature created by the sender's ASI node. This signature contains no personal data but confirms that the message passed through a node trusted by the network. The signature cannot be forged or reproduced outside ASI, because the keys are stored within the infrastructure and are inaccessible to participants. GSI does not analyze the signature but verifies its validity to ensure that the message was indeed created by an authorized node. This eliminates the possibility of request falsification, response substitution, or third-party interference. The cryptographic signature becomes the technical equivalent of an organization's seal, but without revealing its identity. It ensures message immutability and guarantees that it was not modified after transmission.

26.3. Message Authenticity Verification

Message authenticity verification occurs automatically at both the GSI and ASI levels. When a request enters the network, GSI verifies the signature and confirms that it was sent through a valid ASI node. If the signature is invalid, the request is rejected at the transport level and does not enter the feed. The same applies to responses: GSI accepts only those responses that are signed by a valid ASI node. The system does not check message content and does not evaluate its relevance—that is done solely by the customer. But it guarantees that the message is

authentic, unforged, and unaltered. If a customer encounters abuse—for example, receiving a response such as "we have a solution" that turns out to be false—they file a complaint. The responder's ASI node is obligated to revoke the offender's ASI API. If it fails to do so, the customer may independently block the specific responder or the entire node. Thus, message authenticity verification and the complaint mechanism form a self-regulating trust system, in which architecture ensures security and participants ensure interaction quality.

Chapter 27. Spam Protection

27.1. Types of Abuse

Abuse in the GSI infrastructure occurs when a participant uses the system not to solve a task, but to submit irrelevant, false, or misleading responses. Since GSI does not analyze message content, the sole criterion for abuse is the customer's reaction. Any response that does not match the request or contains false promises is considered abuse. The system guarantees sender authenticity and message structural correctness, while quality assessment remains entirely on the customer side.

27.2. Mass Distributions

Mass distributions are impossible due to ASI node architecture. Each response is tied to a specific request, and the sender's ASI node does not permit sending the same response to multiple requests. Attempts at duplicate submission are automatically blocked. This eliminates the possibility of using GSI as a channel for mass promotion or advertising message distribution. The system does not analyze response meaning but guarantees that each response is unique and linked to a specific task.

27.3. Irrelevant Responses

Irrelevant responses are the most common form of abuse among verified participants. If an organization or startup submits a response such as "we have a solution to your problem," and after contact it turns out there is no solution, the customer files a complaint. The complaint is transmitted to the responder's ASI node, and the node is obligated to revoke the offender's ASI API. If the node ignores the complaint, the customer may block the specific responder or the entire node. Blocking means the customer no longer sees responses from that node. Thus, responsibility for interaction quality lies with the participants, while the system provides the technical means to respond to violations.

27.4. Prevention Mechanisms

Abuse prevention mechanisms are based on the separation of interaction channels.

Verified organizational responses are transmitted directly through GSI. The customer may block a specific verified sender or an entire ASI node if the node systematically ignores complaints.

Anonymous responses—from organizations, startups, and individuals—pass through the ASI node, which applies uniform filtering mechanisms, structure verification, and flow limitations. Junk or irrelevant responses are filtered out at this level and do not reach the customer. Blocking an anonymous sender is impossible and unnecessary, as filtering already provides protection against abuse.

Additionally, an organization may completely disable the option to receive anonymous responses when creating a request. This is not a blocking mechanism but a visibility setting: the customer chooses whether they want to see proposals from anonymous participants or prefer to work only with verified ones.

Thus, the GSI architecture combines openness with filtering mechanisms and flexible settings, enabling participants to interact freely while preventing abuse and preserving system resilience.

Chapter 28. Complaints and Responsibility

28.1. Submitting a Complaint

A complaint is the primary mechanism for protecting a customer against abuse in the GSI infrastructure. If a customer receives a response that violates interaction rules, contains false promises, or is used to promote third-party services, they may file a complaint through their ASI node. A complaint always pertains to a specific response and is recorded by the system as a formal violation notice. GSI does not analyze complaint content and does not make decisions; it merely transmits the complaint to the sender's ASI node. Filing a complaint does not require explanations or evidence—the customer determines for themselves whether a response constitutes abuse. This makes the mechanism simple, fast, and fully controlled by participants.

28.2. Violation Review

Violation review occurs at the sender's ASI node level. It is the node that is responsible for its clients' behavior and decides on the consequences. If a complaint

confirms a violation, the ASI node revokes the sender's access to the ASI API, making further participation in GSI on behalf of that organization or startup impossible. The decision is made by the node automatically or manually, depending on the ASI operator's internal policies. GSI does not intervene in this process and does not regulate it. If an ASI node ignores complaints or systematically fails to respond to violations, the customer may block that node at their own level. Blocking means the customer no longer sees requests and responses passing through that node and entirely excludes interaction with it.

28.3. Participant Responsibility

Participant responsibility in GSI is built on the principle of a direct link between behavior and consequences. Verified organizations and startups bear full responsibility for their responses: if they submit irrelevant solutions, mislead the customer, or use the system for promotion, they lose access to the ASI API. This makes abuse economically and reputationally unviable.

Individuals also bear responsibility for their actions, but their participation is limited to the ASI channel, which does not permit mass abuse.

Anonymous responses—from organizations, startups, and individuals—pass through the unified ASI channel with filtering that screens out junk and irrelevant responses. Blocking an anonymous sender is impossible, since even the ASI node does not know the sender's identity, and it is unnecessary because filtering already provides protection. An organization may additionally disable receiving anonymous responses at the request level if it wants to work only with verified participants.

Thus, responsibility is distributed between verified participants and their ASI nodes, while the system remains resilient and self-regulating.

28.4. The Role of ASI Nodes

ASI nodes play a key role in ensuring trust and security within GSI. They verify the authenticity of requests and responses, control the structural correctness of messages, and bear responsibility for the behavior of their verified clients. The ASI node is the only level that can revoke a verified organization's access to the ASI API, thereby excluding it from interaction.

For anonymous responses, the ASI node provides a unified channel for filtering and structuring, screening out junk and irrelevant responses before they reach the customer. The ASI node does not know the identity of an anonymous sender, so blocking anonymous senders is impossible and unnecessary.

Thus, ASI nodes form the foundation of trust in GSI, ensuring authenticity, filtering, responsibility, and resilience for the entire ecosystem.

Chapter 29. Local Blocking of Participants

29.1. Blocking Companies

Local blocking of companies is a tool that enables the customer to manage their own interaction perimeter within GSI. If a verified company violates rules, submits irrelevant responses, or uses the system for unintended purposes, the customer may block it through their ASI node. Blocking operates bidirectionally: the customer no longer sees responses from that company, and the company no longer sees the customer's requests. This excludes any further interaction attempts and establishes a clear boundary between participants. The block is local and does not affect the company's operation within the broader system.

29.2. Blocking Organizations

Blocking organizations follows the same principles as blocking companies but applies to a broader range of participants—startups, research centers, universities, and other entities. If an organization systematically violates rules or submits irrelevant responses, the customer may locally block it. After blocking, the organization no longer sees the customer's requests, and the customer no longer sees its responses. This creates a bidirectional barrier that excludes any further contact. The block is not recorded globally and does not affect the organization's interaction with other GSI participants.

29.3. Blocking ASI Nodes

If violations are systemic and related not to an individual organization but to the behavior of an entire ASI node, the customer may block the node itself. This is an extreme measure applied in cases where a node ignores complaints, fails to revoke API access for violators, or permits mass abuse. Node blocking also operates bidirectionally: the customer no longer sees responses and requests passing through that node, and the node no longer sees the customer's requests. This completely excludes interaction between the parties and establishes a clear trust perimeter. The block remains local and does not affect the node's operation in the global network.

29.4. Consequences of Blocking

The consequences of blocking are always limited to the specific participant. A blocked company, organization, or ASI node loses the ability to interact with the customer who applied the block and ceases to see their requests. The customer, in turn, no longer receives responses from blocked participants. A block is not a global penalty and does not affect participants' operation in the broader system. It serves as a tool for managing interaction quality and enables each organization to form its own trust perimeter. Thanks to the bidirectional nature of blocking, any attempts to circumvent or re-establish contact are excluded, and interaction remains transparent, predictable, and secure.

Chapter 30. Self-Isolation of Violators as a Market Mechanism

30.1. Federated Trust Model

Self-isolation of violators in the GSI infrastructure emerges naturally through the federated trust model, in which each organization independently determines with whom it is willing to interact. ASI nodes do not form a single control center and do not impose global blocking rules. Instead, each company builds its own trust perimeter based on interaction experience and the quality of responses received. If a participant violates rules, submits irrelevant responses, or misleads others, they gradually lose access to requests from an increasing number of organizations. This is not an administrative measure but a natural market process: trust is formed locally, and its loss leads to the violator's self-isolation.

30.2. Organizational Reputation Beyond GSI

Organizational reputation in GSI is formed not only within the network but also beyond it. Companies that systematically violate rules quickly lose the ability to participate in projects, partnerships, and joint developments. Since GSI serves as an entry point for interaction between organizations, startups, and research entities, loss of trust within the network reflects on their position in the real market. Verified participants who demonstrate high-quality responses and adhere to collaboration terms, conversely, strengthen their reputation and gain access to a greater number of requests. Thus, GSI becomes not only a transport protocol but also a mechanism for shaping market reputation.

30.3. Loss of Access to Interaction

Loss of access to interaction is a direct consequence of violations. If an organization submits false or irrelevant responses, customers block it locally, and it ceases to see their requests. Blocking operates bidirectionally: the customer does not see the violator's responses, and the violator does not see the customer's requests. When such blocks accumulate, the organization finds itself in a situation where its access

to requests is significantly restricted. This leads to effective self-isolation: the organization remains formally present in GSI, but its ability to participate in interaction sharply declines. Loss of access becomes an economic incentive to comply with rules and maintain high-quality responses.

30.4. Network Self-Regulation

Network self-regulation is based on the principle that GSI does not impose global sanctions and does not manage participant reputation. All decisions are made locally, at the level of individual organizations and their ASI nodes. If a participant behaves correctly, they gain access to a broad range of requests and partnerships. If they violate rules, they gradually lose trust and become isolated. This model does not require centralized moderation, complex algorithms, or global blacklists. The network regulates itself because every participant has a stake in interaction quality. As a result, GSI remains an open, flexible, and resilient infrastructure in which market mechanisms naturally maintain order and trust.

Chapter 31. Abuse Protection Through Complaints

31.1. False Complaints

A complaint in the GSI infrastructure is not a tool of pressure or a means to restrict competitors. It does not affect the violator's access to other participants and does not create any advantages for the complainant. Any company may at any time locally block another participant, and no complaint is required for that. Therefore, a false complaint provides no benefit to the complainant and cannot be used as a mechanism for competitive warfare. A complaint serves exclusively as a signal to the ASI node that one of its clients is violating interaction rules. If no violation exists, the complaint simply does not lead to action, and participant operations remain unaffected.

31.2. Competitive Attacks

Since a complaint does not restrict the violator's access to other companies and does not affect their standing in the system, it cannot be used as a tool for competitive attacks. A company wishing to cease interaction with a competitor may do so directly through local blocking, without resorting to complaints. A complaint does not block a participant globally and does not create reputational consequences for them outside the specific ASI node. Thus, the system excludes the possibility of using complaints for pressure, manipulation, or attempts to eliminate competitors. A

complaint remains a mechanism of internal quality control, not a tool of confrontation.

31.3. Balance of Participant Interests

Balance of interests is achieved because a complaint is not a mandatory element of interaction. A company may choose not to file a complaint at all and simply block the violator locally. A complaint is used only when a company wishes not merely to cease interaction but to prevent further violations by a specific participant against other companies. This makes the complaint a mechanism of collective protection rather than individual pressure. The ASI node receives a signal about a violation and makes a decision in the interest of all its clients, preserving the node's quality and reputation.

31.4. Principles of Fairness

Fairness is ensured because a complaint is not a sanction in itself. It does not lead to automatic consequences and does not restrict a participant globally. The decision is made by the ASI node, which is responsible for its clients and for the quality of interaction. If the violation is confirmed, the node revokes the violator's access to the ASI API, thereby protecting all other participants. If no violation exists, the complaint does not lead to action. This approach excludes abuse, preserves freedom of choice for each company, and maintains high interaction quality within the network. A complaint becomes a tool of self-regulation rather than a means of pressure, making the system resilient, fair, and protected against manipulation.

Chapter 32. Anonymous Interaction

32.1. Reasons for Anonymity

Anonymous mode in the GSI infrastructure is designed for situations where a participant cannot disclose their organizational affiliation due to legal, regulatory, or corporate reasons. It enables companies and individuals to share solutions without entering into formal relationships. Anonymity does not create hidden channels: every anonymous response passes through an ASI node, which processes and structures it while ensuring interaction correctness. However, the ASI node does not know the identity of the anonymous sender—it only verifies structural integrity and applies filtering rules. To the customer, an anonymous response appears identical regardless of whether it was sent by an organization or an individual. This makes anonymous mode safe, predictable, and convenient for participants who need to preserve confidentiality.

32.2. International Restrictions and Regulatory Barriers

In a global environment, companies often face legal and regulatory constraints that limit their ability to formally interact with foreign organizations. Anonymous mode enables participants to share knowledge and technologies without violating corporate policies or international regulations. Since the customer does not see who submitted the anonymous response, and the interaction passes through the ASI node with structural verification but without identity disclosure, the system remains neutral and does not create risks for participants. GSI is not a tool for circumventing laws; it provides a secure channel for knowledge exchange under complex international rules, preserving transparency and predictability for all parties.

32.3. Free Assistance and Solution Disclosure

Anonymous mode is used in situations where a participant wants to provide a solution free of charge, without contract execution and without disclosing their identity. This is important for research groups, independent specialists, and organizations that wish to share knowledge without entering into formal relationships. An anonymous response is a one-way contribution to solving a task and does not imply further negotiations. This approach enables participants to share experience and technologies without creating obligations and without violating internal policies. Anonymity makes this process safe, and passage through the ASI node ensures structural correctness and quality of interaction, even though the node does not know the sender's identity.

32.4. Limitations of Anonymous Mode

Anonymous mode has clear limitations that ensure system security and resilience. An anonymous participant cannot conduct negotiations, conclude deals, or engage in prolonged interaction—they may only provide a solution. An anonymous response does not build reputation and does not create an interaction history: each submission is independent of previous ones. This excludes the possibility of using anonymity for pressure, manipulation, or hidden influence. Since every anonymous response passes through the ASI node with structural verification and filtering, the customer receives only correctly formatted responses that meet quality standards—even though the node does not know who the sender is. This approach makes GSI a supranational infrastructure comparable in openness to the Internet, yet secure and predictable for all participants.

Chapter 33. Growth in the Number of ASI Nodes

33.1. Emergence of Multiple Independent ASI Nodes

The growth in the number of independent ASI nodes is a natural stage in the infrastructure's evolution. As companies, universities, and research centers begin using ASI for idea filtering and interaction, the need arises to create their own nodes that reflect their internal standards, processes, and requirements. Each node becomes an independent operator that defines access rules, manages clients, and ensures interaction quality. The emergence of multiple independent ASI nodes does not lead to fragmentation—on the contrary, it creates diversity of approaches and strengthens the ecosystem's resilience. Each node becomes an entry point into the innovation environment, and their collective forms a distributed network with no center and no single point of failure.

33.2. Evolution of Innovation Ecosystems

The emergence of multiple ASI nodes leads to the formation of local innovation ecosystems, each evolving according to its own rules. Companies cluster around nodes that match their culture, industry, or maturity level. Universities create nodes for research projects, startups for rapid experimentation, large corporations for internal processes. These ecosystems do not compete with one another; they complement each other, creating a multi-layered interaction structure. The growth in the number of nodes accelerates knowledge exchange, improves idea filtering quality, and makes the innovation process more flexible. As a result, ASI ceases to be a tool of a single company and transforms into the foundation of a distributed innovation environment.

33.3. The Need for a Common Infrastructure

When the number of ASI nodes reaches a critical mass, the need arises for a common infrastructure that enables them to interact with one another. Nodes must be able to exchange requests, transmit responses, verify message authenticity, and ensure format compatibility. This role belongs to GSI—a supranational infrastructure that unites independent ASI nodes into a single network. GSI does not manage the nodes and does not interfere with their internal processes; it provides the transport layer that allows them to interact without centralized control. As a result, ASI nodes retain autonomy while gaining the ability to operate in a global environment where every idea can be heard and every solution can be found. The common infrastructure becomes a natural continuation of ASI growth and ensures the scalability of the entire ecosystem.

Chapter 34. Compatibility Between ASI Operators

34.1. Interaction Standards

Compatibility between ASI operators is ensured by unified interaction standards that define request structure, response format, and routing rules. These standards do not regulate operators' internal processes and do not restrict their freedom, but they establish the minimum level of technical consistency necessary for operation within the shared network. Each operator may use their own models, their own filtering methods, and their own registration rules, but must support a unified data exchange format. As a result, nodes remain fully independent yet capable of interacting with one another through GSI without creating barriers or incompatibilities. Interaction standards form the foundation of a distributed infrastructure in which each node retains autonomy while remaining part of a unified space.

34.2. Federated Compatibility

Federated compatibility means that each ASI operator functions as an independent system while being able to interact with other nodes without centralized management. Nodes are not required to trust one another directly: trust is facilitated through GSI, which verifies the authenticity of requests and responses but does not interfere with their content. This model enables operators to maintain their own quality standards, their own access rules, and their own moderation mechanisms without compromising compatibility with other network participants. The federated structure makes the system scalable: new nodes may connect without coordination with existing ones, and existing nodes may evolve independently. As a result, the ASI ecosystem grows organically, without centralization and without the need for global governance.

34.3. Independence and Collaboration

Independence of ASI operators does not exclude collaboration—on the contrary, it makes it more flexible and natural. Each node defines its own rules but may accept requests and responses from other nodes if they conform to common standards. This creates an environment in which operators compete on quality, speed, and convenience, but do not block one another and do not create closed ecosystems. Collaboration emerges where it benefits participants, and independence enables each node to evolve in its own direction. GSI provides the transport layer that connects these independent systems into a unified network, maintaining a balance between operator freedom and the necessary degree of compatibility. As a result, ASI remains an open, distributed, and resilient infrastructure capable of supporting global interaction without centralization.

Chapter 35. Global Network of Innovation Interaction

35.1. A Fully Formed Ecosystem

When the number of independent ASI nodes reaches a critical mass, the ecosystem ceases to be a collection of separate operators and transforms into a global network of innovation interaction. Each node serves its own audience, but all are linked by unified standards and the GSI transport layer. In such an environment, ideas, solutions, and requests flow freely between organizations, universities, startups, and research centers, regardless of their geography and internal structure. The ecosystem becomes self-sustaining: new participants connect to existing nodes, nodes evolve and specialize, and the network as a whole remains resilient due to its distributed architecture. This is not a centralized system but an organically growing infrastructure in which every point strengthens the entire network.

35.2. Organizations as Nodes of the Global Network

In a fully formed ecosystem, each organization becomes a node of the global network—not merely a consumer of solutions but also a source of knowledge. Companies, research groups, and startups participate in the exchange of ideas through their ASI nodes, which provide filtering, structuring, and routing of interactions. An organization may simultaneously act as customer, implementer, and observer, while maintaining control over its own data and internal processes. Nodes do not compete for control over the network; they compete on filtering quality, processing speed, and interaction convenience. This creates a natural development dynamic: strong nodes attract more participants, weak ones adapt or disappear. As a result, each organization becomes part of the global innovation fabric, retaining autonomy and gaining access to the world's intellectual resource.

35.3. New Models of Collaboration

The global network of innovation interaction opens new models of collaboration that were previously impossible. Organizations may unite around complex tasks without formal agreements and without creating temporary consortia. Startups may find solutions for large corporations without entering into direct contact. Universities may share research results without disclosing internal structures. Anonymous mode allows participants to provide knowledge without formal obligations, while open mode enables long-term partnerships. GSI provides the transport layer that makes these models possible, and ASI nodes provide the intellectual layer that makes them effective. As a result, a new form of global collaboration emerges: distributed, flexible, and knowledge-based rather than formal-structure-based. This collaboration

does not require centralization, because the network itself ensures resilience and interaction quality.

Chapter 36. From Accelerating Solution Discovery to Accelerating Progress

36.1. Reducing Communication Barriers

The emergence of a distributed network of ASI nodes and the GSI transport layer radically reduces communication barriers between organizations. Previously, finding a solution required lengthy negotiations, approvals, legal procedures, and trust-building. In GSI, these barriers disappear: a request instantly becomes available to thousands of organizations, and responses arrive directly, without intermediaries and without the need to form relationships in advance. This does not merely accelerate communication—it changes its nature. Interaction becomes event-driven rather than contract-driven: a solution arrives when it is found, not when the parties have managed to reach an agreement. Such an approach makes the innovation process continuous and reduces the cost of solution discovery to the minimum possible level.

36.2. Accelerating Technology Adoption

The reduction of communication barriers leads to accelerated technology adoption. Organizations gain access to solutions faster than they can form internal teams or engage external contractors. Startups can offer technologies to large corporations without complex procedures, and research groups can share results without waiting for publications or formal agreements. GSI transforms innovation from a linear process into a parallel one: multiple organizations simultaneously work on tasks, and each gains access to the best solutions regardless of its size or resources. This creates an acceleration effect: the more participants are connected, the faster technologies spread, and the faster they move from idea to implementation.

36.3. The Global Effect of GSI

The global effect of GSI manifests in the network's ability to unite local innovation ecosystems into a single structure. ASI nodes operating in different countries, industries, and scientific fields become parts of a common network in which knowledge spreads without geographical or organizational constraints. This creates a "global intelligence" effect: every organization gains access to the world's pool of solutions, and every idea can be applied where it is most valuable. GSI does not replace existing institutions—it complements them, creating an interaction layer that

operates faster, more flexibly, and at greater scale. As a result, innovation ceases to be a local phenomenon and becomes a global process accessible to every network participant.

36.4. Long-Term Impact on Civilizational Development

The long-term impact of GSI extends beyond accelerating individual processes. When solution discovery becomes instantaneous and technology adoption becomes continuous, the very dynamics of civilizational development change. Progress ceases to depend on chance encounters, rare collaborations, or limited resources. It becomes a systemic property of the infrastructure, in which every task automatically finds those capable of solving it. This creates a new level of resilience: even small organizations can contribute to global development, while large ones gain access to the best ideas regardless of their origin. In such an environment, innovation becomes not the exception but the norm, and progress becomes a natural consequence of the distributed network's operation. GSI transforms civilizational development into a continuous process in which knowledge and solutions circulate as freely as information on the Internet.

Conclusion

The development of the ASI infrastructure and the emergence of the supranational GSI layer demonstrate that innovation is no longer a localized process confined to the resources of individual companies or research groups. It becomes a property of the environment—distributed, resilient, and open. In such an environment, every organization gains the ability to find solutions faster than barriers can arise, and every idea can be heard regardless of its origin.

This book describes neither a technology nor a platform. It describes an interaction architecture in which solution discovery becomes a natural consequence of the network's structure. ASI nodes provide filtering, routing, and trust, while GSI creates the space in which these nodes can work together without losing autonomy. The result is a new form of collaboration—flexible, distributed, and knowledge-based rather than formal-relationship-based.

The primary value of this architecture lies in the fact that it does not require centralization. It grows organically, like the Internet, and maintains resilience through the multiplicity of independent participants. Each node strengthens the network, each organization contributes to collective progress, and every discovered idea becomes part of the global intellectual space. This does not abolish existing

institutions—on the contrary, it complements them, creating an interaction layer that operates faster and at greater scale.

GSI does not accelerate innovation by itself. It creates the conditions under which innovation accelerates naturally. When communication barriers disappear and access to knowledge becomes instantaneous, progress ceases to be the result of rare coincidences. It becomes a systemic property of the infrastructure. And in this lies GSI's primary long-term impact: it transforms civilizational development into a continuous process in which every valuable idea has a chance to be heard.

This book is complete, but the architecture itself is not. It will evolve together with its participants, nodes, ecosystems, and new forms of collaboration. GSI is not an endpoint but the beginning of a new era—one in which knowledge becomes accessible, interaction becomes free, and progress becomes natural.

APPENDICES

Appendix A. Example of an Open Request

Below is an example of an open request formatted strictly according to the mandatory structure defined in Chapter 17. All fields conform to the ASI/GSI standard and demonstrate the correct format for publication in the network.

Example Open Request

Request ID:
RQ-2026-00417 (generated by the ASI node upon request creation)

Company ID:
ORG-5821 (assigned upon organization registration through the ASI API)

Problem Statement:
It is necessary to increase the endurance of small unmanned aerial vehicles used for agricultural territory monitoring. The current configuration provides insufficient operational duration under high sensor load.

Requirements Description:
An engineering or architectural solution is required to improve the energy efficiency of onboard systems without increasing battery mass and without reducing the quality of collected data. Hardware, firmware, or system-level approaches aimed at

optimizing power consumption of sensors, computing modules, or power distribution circuits are acceptable. The solution must be described in sufficient detail to assess its applicability in series production.

Constraints and Evaluation Criteria:
The solution must not increase device mass, require scarce components, or alter the aircraft's intended purpose. Options involving replacement of the battery with a heavier or non-standard unit are not considered. Expected endurance improvement: 15% to 25%. Solutions that do not require major structural modifications are preferred.

Collaboration Terms:
Pro bono participation (public disclosure of the solution). Responses may be verified or anonymous. Further interaction is possible only at the customer's initiative following analysis of received solutions.

Additional Parameters:

- Battery type: Li-ion, 3S, 2200 mAh
- Sensors: multispectral camera (5 channels), GPS module, microclimate sensors
- Current power consumption: ~45 Wh at full load
- Optimizations already implemented: software power management (~7% improvement)
- Disclosure restrictions: structural drawings and power supply schematics are not disclosed

Appendix B. Example of a Directed Request

A directed request is used when the customer directs a task to a specific organization through its ASI node. Such a request is not published in the public feed and is accessible only to the intended recipient. The structure fully conforms to the standard described in Chapter 17.

Example Directed Request

Request ID:
RQ-2026-01844 (generated by the ASI node upon request creation)

Customer Company ID:
ORG-5821

Recipient Company ID:
ORG-9920 (specified by the customer when creating the directed request)

Problem Statement:
It is necessary to develop a compact video stream stabilization module for small unmanned aerial vehicles. The current stabilization system relies on software post-processing and does not provide sufficient image quality under gusty wind conditions and airframe vibrations.

Requirements Description:
A hardware-software solution is required that enables real-time video stream stabilization. The module must compensate for vibrations, short-term jerks, and camera micro-drift. An architectural description, computational resource requirements, expected image stability improvement, and possible integration options into the existing platform must be provided.

Constraints and Evaluation Criteria:
The solution must operate on the existing hardware platform without increasing mass by more than 20 grams. Video stream processing latency must not exceed 30 ms. Solutions requiring camera replacement or modification of the gimbal design are not acceptable. Expected image stability improvement: no less than 40% compared to the current system.

Collaboration Terms:
Interaction format is closed. The response must be verified. Subsequent commercial integration is possible following technical evaluation of the solution. Anonymous responses are not permitted in directed requests.

Additional Parameters:

- Current camera: 1080p, 60 fps
- Processor: ARM Cortex-A53, 1.2 GHz
- Permissible module power consumption: no more than 3.5 W
- Additional data: the customer is prepared to provide test video recordings, vibration profiles, and gimbal parameters
- Disclosure restrictions: source code of the current stabilization software is not provided

Appendix C. Example of a Response to a Request

Below is an example of a correctly formatted response to an open request, conforming to the structure defined in Chapter 17. The response is submitted on behalf of the implementing organization and contains a technical description of the proposed solution.

Example Response to a Request

Response ID:
RS-2026-02791 (generated by the ASI node upon response submission)

Implementing Company ID:
ORG-7744

Solution Summary:
We propose the implementation of a hybrid adaptive power management system for the sensor module, based on dynamic sensor polling frequency adjustment and intelligent distribution of computational load. The solution enables a 16–22% increase in UAV endurance without altering battery mass.

Approach Description:
The system employs a model for evaluating contextual flight parameters (speed, altitude, illumination, data density, battery status) and adjusts sensor operating modes accordingly. The multispectral camera is switched to variable frame rate mode, the GPS module to adaptive coordinate update mode, and the microclimate sensors to batch polling mode. The algorithm runs on the embedded ARM Cortex-A53 processor and utilizes a lightweight decision model with latency under 40 ms. The expected effect is achieved by reducing redundant measurements and optimizing computational load distribution among modules.

Constraints and Applicability:
The solution requires no structural modifications and is compatible with the existing hardware platform. Minimal firmware updates to the sensor module are required. Solution effectiveness depends on illumination stability and mission profile: maximum effect is achieved during extended flights under varying conditions. Not suitable for UAVs operating under persistent high turbulence.

Additional Parameters:

- Testing conducted on a platform with a 3S 2200 mAh battery and standard sensor suite

- Average sensor module power consumption reduction: 12–14%
- A set of test logs demonstrating algorithm performance across various scenarios is provided
- Source code is not provided, but API-based integration is possible

Appendix D. Example of an Individual's Response in Open and Free Mode

An individual's response in open mode is used when a network participant wishes to share a solution free of charge and without disclosing their identity. The ASI node conceals the sender's data, verifies format correctness, and ensures identity protection.

The customer sees only the technical content of the response and the identifier of the ASI node through which it was sent.

The structure fully conforms to the standard described in Chapter 17.

Example of an Individual's Response Through ASI (Open Free Mode)

Response ID:
RS-2026-04112 (generated by the ASI node upon response submission)

ASI Node ID:
ASI-NODE-1442 (the node through which the individual submitted the response; sender identity is concealed)

Solution Summary:
I propose using an adaptive method of reducing the multispectral camera's operating frequency during stable flight periods. This reduces camera power consumption without noticeable degradation of data quality and increases UAV endurance.

Approach Description:
The method is based on flight dynamics analysis: if speed, heading, and illumination remain stable, the camera automatically switches to reduced frame rate mode. When conditions change, the frequency returns to standard level. Additionally, local frame filtering on the sensor module's microcontroller is proposed, which reduces the volume of data transmitted to the main processor. In tests on a similar platform,

camera power consumption reduction was 9–12%, yielding a 6–8% increase in flight time.

Constraints and Applicability:
The method is suitable for missions with extended straight-line segments and stable illumination. Not suitable for tasks requiring constant high frame rate. Requires no structural modifications but does require camera firmware updates. Effectiveness depends on mission profile and lighting conditions.

Additional Parameters:

- Testing conducted on a platform with a 3S 2200 mAh battery
- Multispectral camera with 5 channels used
- Algorithm implemented on STM32F4 microcontroller
- Source code not provided; pseudocode transfer through ASI is possible
- The sender uses open free mode and makes no claim to compensation

Appendix E. GSI Protocol Message Formats (Text Version)

The GSI protocol defines a unified message exchange format between ASI nodes, organizations, and individuals. All messages have a strict structure that ensures routing, verification, identity protection, and compatibility among network participants. Each GSI message is a structured object with mandatory fields defined by the standard. ASI nodes verify format correctness, field validity, and compliance with security policy.

E.1. General GSI Message Structure

Any message in the GSI protocol has the following base framework:

```
text

type: <message_type>
version: 1.0
timestamp: <ISO-8601>
payload: { substantive content }
meta:
  - asi_node_id: <ASI node ID>
  - signature: <cryptographic signature>

  - routing: delivery service parameters
```

Mandatory elements:

- `type` — message type (request, response, complaint, acknowledgment, etc.)
- `version` — protocol version
- `timestamp` — time of sending
- `payload` — substantive content
- `meta` — service information for ASI

E.2. Request Message Format

Used for publishing open and directed requests.

```
text
```

```
type: request
version: 1.0
timestamp: <ISO-8601>
payload:
  - request_id: <request ID>
  - company_id: <company ID>
  - target_company_id: <recipient ID or null>
  - problem: problem statement
  - requirements: requirements description
  - constraints: constraints and evaluation criteria
  - cooperation: collaboration terms
  - extra: additional parameters
meta:
  - asi_node_id: <ASI node>
  - signature: <signature>
  - routing:
      visibility: open or direct
      priority: normal or high
```

Features:

- `target_company_id = null` for open requests
- `visibility = direct` for directed requests
- `extra` may contain any additional parameters

E.3. Response Message Format

Used by organizations and individuals.

```
text
```

```
type: response
version: 1.0
timestamp: <ISO-8601>
payload:
  - response_id: <response ID>
  - request_id: <request ID>
  - sender_type: company or individual
  - company_id: <company ID or null>
  - solution: solution summary
  - approach: approach description
  - limitations: constraints and applicability
  - extra: additional parameters
meta:
  - asi_node_id: <ASI node>
  - signature: <signature>
  - routing:
      visibility: open
      mode: free or paid
```

Features:

- `company_id = null` for individuals
- ASI conceals sender identity
- `mode = free` for free open mode

E.4. Complaint Message Format

Used for disputing violations, spam, or incorrect responses.

```
text
```

```
type: complaint
version: 1.0
timestamp: <ISO-8601>
payload:
  - complaint_id: <complaint ID>
  - related_id: <request or response ID>
  - reason: violation description
  - details: additional information
meta:
```

```
  - asi_node_id: <ASI node>
  - signature: <signature>
  - routing:
      visibility: private
```

E.5. Acknowledgment Message Format

Used by ASI nodes to confirm delivery, verification, or rejection.

```
text

type: ack
version: 1.0
timestamp: <ISO-8601>
payload:
  - related_id: <request/response/complaint ID>
  - status: accepted, rejected, or delivered
  - info: additional details
meta:
  - asi_node_id: <ASI node>
  - signature: <signature>
```

E.6. System Notification Message Format

Used for protocol updates, warnings, or policy changes.

```
text

type: system
version: 1.0
timestamp: <ISO-8601>
payload:
  - category: policy, update, or warning
  - message: notification text
meta:
  - asi_node_id: ASI-CORE
  - signature: <signature>
```

E.7. Cryptographic Signature Requirements

Every message is signed with the ASI node's key using the algorithm defined by the standard. The signature ensures message immutability, sender identity protection, and trust between nodes.

E.8. Routing Rules

ASI nodes use the `visibility`, `target_company_id`, and `priority` fields to determine:

- who receives the message,
- how it is delivered,
- and in what order.

Appendix F. ASI Node Responsibility Policy

The ASI Node Responsibility Policy defines the obligations, limitations, and guarantees that ensure the correct operation of the global GSI network. Each ASI node acts as a trusted intermediary between authors, organizations, and the GSI protocol, ensuring security, identity protection, format correctness, and standards compliance.

No ASI node is the owner of data, ideas, or solutions. The node performs strictly defined functions aimed at maintaining the integrity and resilience of the infrastructure.

F.1. ASI Node Obligations

Each ASI node is obligated to:

1. Verify the structural correctness of all incoming messages according to the GSI standard.
2. Provide cryptographic signature for all outgoing messages.
3. Guarantee the protection of identity for individuals submitting responses or requests in open mode.
4. Ensure message routing in accordance with protocol rules.
5. Filter spam, malicious messages, and policy violations.
6. Store the minimum necessary service information required for protocol operation.
7. Ensure the immutability and integrity of transmitted data.

8. Maintain an up-to-date version of the protocol and security policy.
9. Ensure transparency of node operations within the limits defined by the protocol.
10. Notify the network of critical errors, failures, or violations.

F.2. ASI Node Liability Limitations

The ASI node is not liable for:

1. The content of ideas, requests, or responses submitted by users.
2. The technical feasibility, quality, or reliability of solutions provided by network participants.
3. Commercial relationships between organizations and authors.
4. Legal consequences of implementing ideas outside the GSI infrastructure.
5. Violations committed by users outside the GSI protocol.
6. Interpretation or evaluation of ideas — this is a function of the semantic core and analysts.
7. Long-term data storage — the node stores only service metadata.

F.3. ASI Node Guarantees

Each ASI node guarantees:

1. Protection of identity for individuals using open free mode.
2. No transfer of personal data to customers or organizations.
3. Inability to disclose the sender's identity without their consent.
4. Cryptographic protection of all messages.
5. Neutrality and non-interference in message content.
6. Compliance with security and filtering policies.
7. Conformance to the GSI standard and compatibility with other nodes.

F.4. Filtering and Moderation Policy

The ASI node is obligated to reject messages containing:

1. Spam, advertising, or mass distributions.
2. Malicious code, hacking attempts, or interference with network operations.
3. Insults, threats, discrimination, or toxic behavior.
4. Attempts to disclose the identity of other participants.

5. Non-compliance with the GSI protocol format.
6. Attempts to circumvent restrictions or violate security policy.

Rejected messages receive status `rejected` with the reason indicated.

F.5. Identity Protection Policy

For individuals using open free mode:

1. The sender's identity is concealed from all network participants.
2. The customer sees only the ASI node ID through which the response was sent.
3. The ASI node does not disclose the sender's identity even upon organizational request.
4. The ASI node stores the minimum data set necessary for abuse protection.
5. The ASI node is not permitted to use sender data outside the GSI protocol.

F.6. Service Refusal Policy

The ASI node has the right to temporarily restrict user access if:

1. The user systematically violates rules.
2. The user sends malicious messages.
3. The user attempts to bypass filters or restrictions.
4. The user creates excessive load on the node.

Restrictions must be proportionate to the violation and documented.

F.7. Protocol Update Policy

The ASI node is obligated to:

1. Maintain an up-to-date version of the GSI protocol.
2. Automatically apply security updates.
3. Notify the network of critical changes via system messages.
4. Ensure compatibility with previous protocol versions during the transition period.

F.8. Transparency Policy

The ASI node is obligated to provide:

1. System error logs (without personal data).
2. Statistics of rejected messages.
3. Information on protocol and policy versions.
4. Description of applied filters and moderation criteria.

Appendix G. Risks, Limitations, and Open Questions of GSI

Despite the architectural completeness and formal rigor of the GSI protocol, the system remains an evolving infrastructure. Below are the key risks, limitations, and open questions that must be considered when designing, implementing, and operating the global semantic innovation network.

G.1. Technical Risks

1. Scalability of the Semantic Core
   The growing volume of ideas may exceed the current capabilities of semantic AI.
   Problem: the need for continuous increases in computational resources.
   Risk: processing delays, reduced evaluation quality.
2. Consistency of Distributed ASI Nodes
   Nodes operate independently but must maintain a unified standard.
   Risk: version divergence, format incompatibility, routing errors.
3. Dependence on Cryptographic Infrastructure
   Signatures and verification are the foundation of the protocol.
   Risk: algorithm obsolescence, need for key rotation, cryptographic attacks.
4. Resilience to Malicious Messages
   Despite filtering, attempts to bypass detection are possible.
   Risk: node overload, spam attacks, attempts to inject malicious data.

G.2. Organizational Risks

1. Uneven Quality of ASI Nodes
   Different operators may provide varying levels of quality.
   Risk: weak nodes become points of vulnerability.
2. Conflicts of Interest Among Organizations
   Organizations may attempt to influence the evaluation of ideas.
   Risk: pressure on analysts, manipulation attempts.
3. Insufficient Transparency of Local Policies
   Although the protocol is unified, operators may introduce additional rules.
   Risk: network fragmentation, reduced trust.

G.3. Social and Ethical Risks

1. Uneven Access to Infrastructure
   Despite openness, some regions may have limited access.
   Risk: exacerbation of global inequality.
2. Potential for Abuse by Users
   Individuals may submit malicious ideas, provocations, or false data.
   Risk: filter load, reduced stream quality.
3. Impact on Career and Social Trajectories
   GSI may become a tool for talent identification.
   Risk: misinterpretation of profiles, social consequences.

G.4. Architectural Limitations

1. Limited Interpretability of Semantic Models
   Even with explainability, "black zones" remain.
   Limitation: inability to fully explain every decision.
2. Message Format Constraints
   Strict structure improves quality but reduces flexibility.
   Limitation: inability to transmit non-standard data types.
3. Privacy Limitations
   Complete anonymity is impossible—the ASI node must know the sender.
   Limitation: balance between privacy and security.

G.5. Open Questions

1. Global Protocol Standardization
   Who defines updates? How are changes coordinated?
   The question remains open.
2. Long-Term Storage of Ideas and Solutions
   How to store billions of semantic objects?
   How to ensure their evolution?
   Further development is required.
3. Conflict Resolution Mechanisms
   What to do if two ASI nodes provide contradictory solutions?
   How to resolve disputes between organizations?
   Additional protocols are needed.
4. Legal Responsibility for Ideas
   Who owns ideas that pass through GSI?
   How to protect authors?
   How to regulate cross-border innovation flows?
   The question requires international consensus.
5. Ethical Boundaries of Idea Amplification
   Semantic synthesis can create new ideas based on others'.
   Where is the line between amplification and co-authorship?
   There is no universal answer yet.

G.6. Directions for Future Research

1. Development of more interpretable evaluation models.
2. Creation of self-regulation mechanisms for ASI nodes.
3. Formation of international GSI standards.
4. Investigation of network resilience to global failures.
5. Development of conflict resolution protocols.
6. Creation of models for long-term evolution of semantic knowledge.